

PCT/JP2004/002228

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

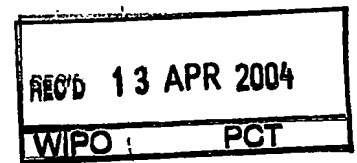
25.2.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2003年 9月 4日

出 願 番 号  
Application Number: 特願2003-312156  
[ST. 10/C]: [J.P.2003-312156]



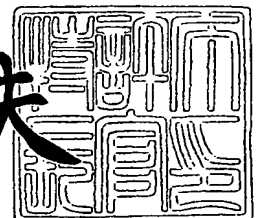
出 願 人  
Applicant(s): 学校法人同志社  
株式会社国際電気通信基礎技術研究所

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 3月26日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号 出証特2004-3025100

【書類名】 特許願  
【整理番号】 1031243  
【提出日】 平成15年 9月 4日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04B 13/00  
【発明者】  
    【住所又は居所】 京都府京田辺市多々羅都谷 1-3 同志社大学内  
    【氏名】 笹岡 秀一  
【発明者】  
    【住所又は居所】 京都府相楽郡精華町光台二丁目 2 番地 2 株式会社国際電気通信  
    基礎技術研究所内  
    【氏名】 青野 智之  
【発明者】  
    【住所又は居所】 京都府相楽郡精華町光台二丁目 2 番地 2 株式会社国際電気通信  
    基礎技術研究所内  
    【氏名】 大平 孝  
【特許出願人】  
    【識別番号】 503027931  
    【住所又は居所】 京都府京都市上京区今出川通烏丸東入玄武町 601 番地  
    【氏名又は名称】 学校法人同志社  
【特許出願人】  
    【識別番号】 393031586  
    【住所又は居所】 京都府相楽郡精華町光台二丁目 2 番地 2  
    【氏名又は名称】 株式会社国際電気通信基礎技術研究所  
【代理人】  
    【識別番号】 100064746  
    【弁理士】  
    【氏名又は名称】 深見 久郎  
【選任した代理人】  
    【識別番号】 100085132  
    【弁理士】  
    【氏名又は名称】 森田 俊雄  
【選任した代理人】  
    【識別番号】 100083703  
    【弁理士】  
    【氏名又は名称】 仲村 義平  
【選任した代理人】  
    【識別番号】 100096781  
    【弁理士】  
    【氏名又は名称】 堀井 豊  
【選任した代理人】  
    【識別番号】 100098316  
    【弁理士】  
    【氏名又は名称】 野田 久登  
【選任した代理人】  
    【識別番号】 100109162  
    【弁理士】  
    【氏名又は名称】 酒井 将行  
【国等の委託研究の成果に係る記載事項】 平成15年度通信・放送機構、研究テーマ「  
自律分散型無線ネットワークの研究開発」に関する委託研究、産  
出証特 2004-3025100

業活力再生特別措置法第 3 0 条の適用を受ける特許出願

【手数料の表示】

【予納台帳番号】

008693

【納付金額】

21,000円

【提出物件の目録】

【物件名】

特許請求の範囲 1

【物件名】

明細書 1

【物件名】

図面 1

【物件名】

要約書 1

**【書類名】 特許請求の範囲****【請求項 1】**

指向性を電氣的に切換え可能な第 1 のアンテナと、  
第 2 のアンテナと、

前記第 1 及び第 2 のアンテナを介して無線伝送路により電波を相互に送受信する第 1 及び第 2 の無線装置とを備え、

前記第 1 の無線装置は、前記第 1 のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第 2 の無線装置から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第 1 の受信信号プロファイルを生成し、その生成した第 1 の受信信号プロファイルに基づいて第 1 の秘密鍵を生成し、

前記第 2 の無線装置は、前記第 1 のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第 1 の無線装置から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第 2 の受信信号プロファイルを生成し、その生成した第 2 の受信信号プロファイルに基づいて前記第 1 の秘密鍵と同じ第 2 の秘密鍵を生成する、無線通信システム。

**【請求項 2】**

前記第 1 及び第 2 の受信信号プロファイルの各々は、前記複数個の指向性に対応した複数の強度からなり、

前記第 1 及び第 2 の無線装置は、前記複数の強度を多値化してそれぞれ前記第 1 及び第 2 の秘密鍵を生成する、請求項 1 に記載の無線通信システム。

**【請求項 3】**

前記第 1 及び第 2 の無線装置は、時分割復信方式により前記複数の電波を送受信する、請求項 1 または請求項 2 に記載の無線通信システム。

**【請求項 4】**

前記第 1 の無線装置は、前記生成した第 1 の秘密鍵が前記第 2 の秘密鍵に一致することを確認する、請求項 1 から請求項 3 のいずれか 1 項に記載の無線通信システム。

**【請求項 5】**

前記第 1 の無線装置は、前記生成した第 1 の秘密鍵が前記第 2 の秘密鍵に不一致であるとき、前記第 1 の秘密鍵を前記第 2 の秘密鍵に一致させる、請求項 1 から請求項 3 のいずれか 1 項に記載の無線通信システム。

**【請求項 6】**

前記第 1 のアンテナは、盗聴者の端末に近接して配置された第 1 の無線装置に設置される、請求項 1 から請求項 5 のいずれか 1 項に記載の無線通信システム。

**【請求項 7】**

前記第 1 及び第 2 の無線装置は、前記第 1 及び第 2 の秘密鍵を用いてデータを暗号及び復号して相互に通信する、請求項 1 から請求項 6 のいずれか 1 項に記載の無線通信システム。

【書類名】明細書

【発明の名称】無線通信システム

【技術分野】

【0001】

この発明は、無線通信システムに関し、特に、暗号化した情報を無線により通信する無線通信システムに関するものである。

【背景技術】

【0002】

最近、情報化社会の発展に伴い情報通信が益々重要になるとともに、情報の盗聴または不正利用がより深刻な問題となっている。このような情報の盗聴を防止するために従来から情報を暗号化して送信することが行なわれている。

【0003】

情報を暗号化して端末間で通信を行なう方式として公開鍵暗号方式と秘密鍵暗号方式とがある。公開鍵暗号方式は、安全性が高いが、大容量のデータの暗号化には向かない。

【0004】

一方、秘密鍵暗号方式は、処理が比較的簡単であり、大容量のデータの高速暗号化も可能であるが、秘密鍵を通信の相手方に送信する必要がある。また、秘密鍵暗号方式は、同一の秘密鍵を使用し続けると、暗号解読の攻撃を受けやすく、安全性が損なわれる可能性がある。

【0005】

そこで、秘密鍵を相手方に送信せずに秘密鍵を共有する方法として、2つの端末間の伝送路の特性を測定し、その測定した特性に基づいて各端末で秘密鍵を生成する方法が提案されている（非特許文献1）。

【0006】

この方法は、2つの端末間でデータを送受信したときの遅延プロファイルを各端末で測定し、その測定した遅延プロファイルをアナログ信号からデジタル信号に変換して各端末で秘密鍵を生成する方法である。即ち、伝送路を伝搬する電波は可逆性を示すために、一方の端末から他方の端末へデータを送信したときの遅延プロファイルは、他方の端末から一方の端末へ同じデータを送信したときの遅延プロファイルと同じになる。従って、一方の端末で測定した遅延プロファイルに基づいて生成された秘密鍵は、他方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵と同じになる。

【0007】

このように、伝送路特性を用いて秘密鍵を生成する方法は、同じデータを2つの端末間で相互に送信するだけで同じ秘密鍵を共有することができる。

【非特許文献1】堀池 元樹、笹岡 秀一、「陸上移動通信路の不規則変動に基づく秘密鍵共有方式」、信学技報、社団法人 電子情報通信学会、2002年10月、TECHNICAL REPORT OF IEICE RCS2002-173, p. 7-12

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかし、2つの端末間で送信されるデータを盗聴者が各端末の近傍で傍受して遅延プロファイルを測定すれば、盗聴者は、各端末で測定した遅延プロファイルに近い遅延プロファイルを取得することができる。その結果、秘密鍵が解読される可能性がある。

【0009】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、秘密鍵の盗聴を抑制可能な無線通信システムを提供することである。

【課題を解決するための手段】

【0010】

この発明によれば、無線通信システムは、第1及び第2のアンテナと、第1及び第2の無線装置とを備える。第1のアンテナは、指向性を電氣的に切換え可能である。第1及び

第2の無線装置は、第1及び第2のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第1の無線装置は、第1のアンテナの指向性が所定のパターンにより複数個に変えられたときに第2の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第1の受信信号プロファイルを生成し、その生成した第1の受信信号プロファイルに基づいて第1の秘密鍵を生成する。また、第2の無線装置は、第1のアンテナの指向性が所定のパターンにより複数個に変えられたときに第1の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第2の受信信号プロファイルを生成し、その生成した第2の受信信号プロファイルに基づいて第1の秘密鍵と同じ第2の秘密鍵を生成する。

【0011】

好ましくは、第1及び第2の受信信号プロファイルの各々は、複数個の指向性に対応した複数の強度からなる。第1及び第2の無線装置は、複数の強度を多値化してそれぞれ第1及び第2の秘密鍵を生成する。

【0012】

好ましくは、第1及び第2の無線装置は、時分割復信方式により複数の電波を送受信する。

【0013】

好ましくは、第1の無線装置は、生成した第1の秘密鍵が第2の秘密鍵に一致することを確認する。

【0014】

好ましくは、第1の無線装置は、生成した第1の秘密鍵が第2の秘密鍵に不一致であるとき、第1の秘密鍵を第2の秘密鍵に一致させる。

【0015】

好ましくは、第1のアンテナは、盗聴者の端末に近接して配置された第1の無線装置に設置される。

【0016】

好ましくは、第1及び第2の無線装置は、第1及び第2の秘密鍵を用いてデータを暗号及び復号して相互に通信する。

【発明の効果】

【0017】

この発明による無線通信システムにおいては、指向性を電氣的に切換え可能な第1のアンテナを介して2つの無線装置間で所定のデータが送受信される。そして、第1のアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが2つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて2つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、2つの無線装置間に形成される伝送路に固有である。即ち、2つの無線装置間で送受信される複数の電波を傍受して受信信号プロファイルを生成しても、その生成した受信信号プロファイルは、2つの端末装置で生成される受信信号プロファイルと異なる。

【0018】

従って、この発明によれば、2つの無線装置において作成される秘密鍵の盗聴を抑制できる。

【発明を実施するための最良の形態】

【0019】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0020】

図1は、この発明の実施の形態による無線通信システムの概略図である。無線通信システム100は、無線装置10、30と、アンテナ11と、アレーアンテナ20とを備える。無線装置10は、例えば、ユーザの移動体通信端末である。また、無線装置30は、例

えば、無線アクセスポイントである。

【0021】

アンテナ11は、無線装置10に装着される。そして、アンテナ11は、全方位性のアンテナである。アレーアンテナ20は、アンテナ素子21～27を備える。アンテナ素子24は、給電素子であり、アンテナ素子21～23、25～27は、無給電素子である。そして、アンテナ素子24は、アンテナ素子21～23、25～27によって取り囲まれている。無給電素子であるアンテナ素子21～23、25～27に装荷された可変容量素子であるバラクタダイオードに印加する直流電圧を制御することにより、アレーアンテナ20は、適応ビーム形成が可能である。

【0022】

即ち、アレーアンテナ20は、無線装置30に含まれるバラクタダイオード（図示せず）に印加する直流電圧を変えることによって指向性を変えられる。従って、アレーアンテナ20は、電氣的に指向性を切換え可能なアンテナである。そして、アレーアンテナ20は、無線装置30に装着される。

【0023】

無線装置10と無線装置30との間で通信が行われる場合、電波は、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間を直接伝搬したり、中間物40による影響を受けて伝搬する。中間物40としては、反射物及び障害物が想定される。中間物40が反射物である場合、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から出射した電波は、中間物40によって反射されて無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬する。また、中間物40が障害物である場合、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から出射した電波は、中間物40によって回折されて無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬する。

【0024】

このように、電波は、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間を直接伝搬したり、中間物40による反射を受けて反射波として伝搬したり、中間物40による回折を受けて回折波として伝搬したりする。そして、電波は、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬する場合、直接伝搬成分、反射波成分及び回折波成分が混在しており、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬した電波がどのような成分により構成されるかによって無線装置10と無線装置30との間の伝送路の特性が決定される。

【0025】

この発明においては、無線装置10と無線装置30との間で通信が行なわれる場合、アレーアンテナ20の指向性を複数個に変えて時分割復信（TDD: Time Division Duplex）により所定のデータが同一の周波数で無線装置10、30間で受信される。そして、無線装置10、30は、アレーアンテナ20の指向性を複数個に変えたときの複数の電波の強度を示す受信信号プロファイルRSSIを生成し、その生成した受信信号プロファイルRSSIに基づいて秘密鍵を作成する。

【0026】

秘密鍵が無線装置10、30において生成されると、無線装置10、30は、生成した秘密鍵により情報を暗号化して相手方へ送信し、相手方から受信した暗号化情報を復号して情報を取得する。

【0027】

図2は、図1に示す一方の無線装置10の概略ブロック図である。無線装置10は、信号発生部110と、送信処理部120と、アンテナ部130と、受信処理部140と、プロファイル生成部150と、鍵作成部160と、鍵一致確認部170と、鍵記憶部180と、鍵一致化部190と、暗号部200と、復号部210とを含む。

## 【0028】

信号発生部110は、秘密鍵を生成するときに無線装置30へ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部120へ出力する。送信処理部120は、変調、周波数変換、多元接続及び送信信号の増幅等の送信系の処理を行なう。アンテナ部130は、図1に示すアンテナ11からなり、送信処理部120からの信号を無線装置30へ送信し、無線装置30からの信号を受信して受信処理部140またはプロファイル生成部150へ供給する。

## 【0029】

受信処理部140は、受信信号の増幅、多元接続、周波数変換及び復調等の受信系の処理を行なう。そして、受信処理部140は、受信処理を行なった信号を必要に応じて鍵一致確認部170、鍵一致化部190及び復号部210へ出力する。

## 【0030】

プロファイル生成部150は、アレーアンテナ20の指向性を複数個に変えたときの複数の電波をアンテナ部130から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部150は、検出した複数の強度からなる受信信号プロファイルRSSIを生成して鍵作成部160へ出力する。

## 【0031】

鍵作成部160は、プロファイル生成部150からの受信信号プロファイルRSSIに基づいて秘密鍵Ks1を作成する。そして、鍵作成部160は、作成した秘密鍵Ks1を鍵一致確認部170及び鍵一致化部190へ出力する。

## 【0032】

鍵一致確認部170は、所定の信号を送信処理部120、アンテナ部130及び受信処理部140を介して無線装置30と送受信し、鍵作成部160によって作成された秘密鍵Ks1が無線装置30において作成された秘密鍵Ks2に一致するか否かを後述する方法によって確認する。そして、鍵一致確認部170は、秘密鍵Ks1が秘密鍵Ks2に一致すると確認したとき、秘密鍵Ks1を鍵記憶部180に記憶する。また、鍵一致確認部170は、秘密鍵Ks1が秘密鍵Ks2に不一致であることを確認したとき、不一致信号NMTHを生成して鍵一致化部190へ出力する。

## 【0033】

鍵記憶部180は、鍵一致確認部170及び鍵一致化部190からの秘密鍵Ks1を記憶する。また、鍵記憶部180は、記憶した秘密鍵Ks1を暗号部200及び復号部210へ出力する。なお、鍵記憶部180は、秘密鍵Ks1を一時的、例えば、無線装置30との通信の間だけ記憶するようにしてもよい。

## 【0034】

鍵一致化部190は、鍵一致確認部170から不一致信号NMTHを受けると、後述する方法によって秘密鍵Ks1を秘密鍵Ks2に一致させる。そして、鍵一致化部190は、一致させた秘密鍵が秘密鍵Ks2に一致することを鍵一致確認部170における方法と同じ方法によって確認する。

## 【0035】

暗号部200は、送信データを鍵記憶部180に記憶された秘密鍵Ks1によって暗号して送信処理部120へ出力する。復号部210は、受信処理部140からの信号を鍵記憶部180からの秘密鍵Ks1によって復号して受信データを生成する。

## 【0036】

図3は、図1に示す他方の無線装置30の概略ブロック図である。無線装置30は、無線装置10のアンテナ部130をアンテナ部220に代え、指向性設定部230を追加したものであり、その他は、無線装置10と同じである。

## 【0037】

アンテナ部220は、図1に示すアレーアンテナ20からなる。そして、アンテナ部220は、送信処理部120からの信号を指向性設定部230によって設定された指向性で無線装置10へ送信し、無線装置10からの信号を指向性設定部230によって設定され



た指向性で受信して受信処理部140またはプロファイル生成部150へ出力する。

#### 【0038】

指向性設定部230は、アンテナ部220の指向性を設定する。また、指向性設定部230は、無線装置10、30において秘密鍵Ks1、Ks2を生成するとき、後述する方法により所定の順序に従ってアンテナ部220の指向性を順次切替える。

#### 【0039】

なお、無線装置30のプロファイル生成部150は、アレーアンテナ20の指向性を複数個に変えたときの複数の電波をアンテナ部220から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部150は、検出した複数の強度からなる受信信号プロファイルRSSIを生成して鍵作成部160へ出力する。

#### 【0040】

図4は、図3に示す指向性設定部230の概略ブロック図である。指向性設定部230は、制御電圧発生回路231と、バラクタダイオード232とを含む。制御電圧発生回路231は、制御電圧CLV1～CLVn（nは自然数）を順次発生し、その発生した制御電圧CLV1～CLVnをバラクタダイオード232へ順次出力する。バラクタダイオード232は、制御電圧CLV1～CLVnに応じて無給電素子であるアンテナ素子21～23、25～27に装荷される容量を変え、アレーアンテナ20の指向性を複数個に順次変える。

#### 【0041】

図5は、図2及び図3に示す鍵一致確認部170の概略ブロック図である。鍵一致確認部170は、データ発生部171と、データ比較部172と、結果処理部173とを含む。なお、無線装置10、30の鍵一致確認部170は、同じ構成からなるが、図5においては、秘密鍵Ks1が秘密鍵Ks2に一致することを確認する動作を説明するために、無線装置30においてはデータ発生部171のみを示す。

#### 【0042】

データ発生部171は、鍵作成部160から秘密鍵Ks1を受けると、秘密鍵Ks1が秘密鍵Ks2に一致することを確認するための鍵確認用データDCFM1を発生し、その発生した鍵確認用データDCFM1を送信処理部120及びデータ比較部172へ出力する。

#### 【0043】

この場合、データ発生部171は、秘密鍵Ks1から非可逆的な演算及び一方向的な演算等により、鍵確認用データDCFM1を発生する。より具体的には、データ発生部171は、秘密鍵Ks1またはKs2のハッシュ値を演算することにより、鍵確認用データDCFM1を発生する。

#### 【0044】

データ比較部172は、データ発生部171から鍵確認用データDCFM1を受け、無線装置30のデータ発生部171で発生された鍵確認用データDCFM2を受信処理部140から受ける。そして、データ比較部172は、鍵確認用データDCFM1を鍵確認用データDCFM2と比較する。データ比較部172は、鍵確認用データDCFM1が鍵確認用データDCFM2に一致するとき、一致信号MTHを生成して結果処理部173へ出力する。

#### 【0045】

また、データ比較部172は、鍵確認用データDCFM1が鍵確認用データDCFM2に不一致であるとき、不一致信号NMTHを生成する。そして、データ比較部172は、不一致信号NMTHを鍵一致化部190へ出力し、不一致信号NMTHを送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

#### 【0046】

結果処理部173は、データ比較部172から一致信号MTHを受けると、鍵作成部160から受けた秘密鍵Ks1を鍵記憶部180へ記憶する。

#### 【0047】

図6は、図2及び図3に示す鍵一致化部190の概略ブロック図である。鍵一致化部190は、擬似シンドローム作成部191と、不一致ビット検出部192と、鍵不一致訂正部193と、データ発生部194と、データ比較部195と、結果処理部196とを含む。

【0048】

なお、無線装置10、30の鍵一致化部190は、同じ構成からなるが、図6においては、秘密鍵 $Ks1$ を秘密鍵 $Ks2$ に一致させる動作を説明するために、無線装置30においては擬似シンドローム作成部191のみを示す。

【0049】

擬似シンドローム作成部191は、鍵一致確認部170のデータ比較部172から不一致信号 $NMTH$ を受けると、鍵作成部160から受けた秘密鍵 $Ks1$ のシンドローム $x_1$ を演算する。より具体的には、擬似シンドローム作成部191は、秘密鍵 $Ks1$ のビットパターン $x_1$ を検出し、ビットパターン $x_1$ に対して検査行列 $H$ を乗算してシンドローム $s_1 = x_1 H^T$ を演算する。そして、擬似シンドローム作成部191は、ビットパターン $x_1$ を鍵不一致訂正部193へ出力し、演算したシンドローム $s_1 = x_1 H^T$ を不一致ビット検出部192へ出力する。

【0050】

なお、これらの演算は、 $\text{mod } 2$ の演算であり、 $H^T$ は、検査行列 $H$ の転置行列である。

【0051】

不一致ビット検出部192は、擬似シンドローム作成部191からシンドローム $s_1$ を受け、無線装置30の擬似シンドローム作成部191によって演算されたシンドローム $s_2 = x_2 H^T$ を受信処理部140から受ける。そして、不一致ビット検出部192は、シンドローム $s_1$ とシンドローム $s_2$ との差分 $s = s_1 - s_2$ を演算する。

【0052】

なお、秘密鍵 $Ks1$ 、 $Ks2$ のビットパターンの差分（鍵不一致のビットパターン）を $e = x_1 - x_2$ とすると、 $s = e H^T$ の関係が成立する。 $s = 0$ の場合、 $e = 0$ となり、秘密鍵 $Ks1$ のビットパターンは、秘密鍵 $Ks2$ のビットパターンに一致する。

【0053】

不一致ビット検出部192は、演算した差分 $s$ が0でないとき（即ち、 $e \neq 0$ のとき）、鍵不一致のビットパターン $e$ を鍵不一致訂正部193へ出力する。

【0054】

鍵不一致訂正部193は、擬似シンドローム作成部191からビットパターン $x_1$ を受け、不一致ビット検出部192から鍵不一致のビットパターン $e$ を受ける。そして、鍵不一致訂正部193は、ビットパターン $x_1$ から鍵不一致のビットパターン $e$ を減算することにより相手方の秘密鍵のビットパターン $x_2 = x_1 - e$ を演算する。

【0055】

このように、鍵一致化部190は、秘密鍵 $Ks1$ 、 $Ks2$ の不一致を誤りと見なして誤り訂正の応用により秘密鍵 $Ks1$ 、 $Ks2$ の不一致を解消する。

【0056】

この秘密鍵を一致させる方法は、鍵不一致のビット数が誤り訂正能力以上である場合に鍵の一致化に失敗する可能性があるので、鍵一致化の動作を行なった後に鍵一致の確認を行なう必要がある。

【0057】

データ発生部194は、一致化後の鍵 $x_2 = x_1 - e$ を鍵不一致訂正部193から受けると、鍵 $x_2$ に基づいて鍵確認用データ $DCFM3$ を発生させ、その発生させた鍵確認用データ $DCFM3$ をデータ比較部195へ出力する。また、データ発生部194は、発生させた鍵確認用データ $DCFM3$ を送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

【0058】

なお、データ発生部194は、鍵一致確認部170のデータ発生部171による鍵確認用データDCFM1の発生方法と同じ方法により鍵確認用データDCFM3を発生する。

**【0059】**

データ比較部195は、データ発生部194から鍵確認用データDCFM3を受け、無線装置30で発生された鍵確認用データDCFM4を受信処理部140から受ける。そして、データ比較部195は、鍵確認用データDCFM3を鍵確認用データDCFM4と比較する。

**【0060】**

データ比較部195は、鍵確認用データDCFM3が鍵確認用データDCFM4に一致するとき、一致信号MTHを生成して結果処理部196へ出力する。

**【0061】**

また、データ比較部195は、鍵確認用データDCFM3が鍵確認用データDCFM4に不一致であるとき、不一致信号NMTHを生成する。そして、データ比較部195は、不一致信号NMTHを送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

**【0062】**

結果処理部196は、データ比較部195から一致信号MTHを受けると、鍵不一致訂正部193から受けた鍵 $x_2 = x_1 - e$ を鍵記憶部180へ記憶する。

**【0063】**

このように、データ発生部194、データ比較部195及び結果処理部196は、鍵一致確認部170における確認方法と同じ方法によって一致化が施された鍵の一致を確認する。

**【0064】**

図7は、受信信号プロファイルRSSIの概念図である。指向性設定部230の制御電圧発生回路231は、各々が電圧 $V_1 \sim V_6$ からなる制御電圧 $CLV_1 \sim CLV_n$ を順次発生してバラクタダイオード232へ出力する。この場合、電圧 $V_1 \sim V_6$ は、それぞれ、アンテナ素子21~23、25~27に装荷される容量を変えるための電圧であり、0~20Vの範囲で変えられる。

**【0065】**

バラクタダイオード232は、パターンP1からなる制御電圧 $CLV_1$ に応じてアレーアンテナ20の指向性のある1つの指向性に設定する。そして、アレーアンテナ20は、設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度 $WI_1$ を検出する。

**【0066】**

次に、バラクタダイオード232は、パターンP2からなる制御電圧 $CLV_2$ に応じてアレーアンテナ20の指向性を別の指向性に設定する。そして、アレーアンテナ20は、設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度 $WI_2$ を検出する。

**【0067】**

以後、同様にして、バラクタダイオード232は、それぞれ、パターンP3~Pnからなる制御電圧 $CLV_3 \sim CLV_n$ に応じてアレーアンテナ20の指向性を順次変える。そして、アレーアンテナ20は、各々設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度 $WI_3 \sim WI_n$ を順次検出する。

**【0068】**

そして、プロファイル生成部150は、強度 $WI_1 \sim WI_n$ からなる強度プロファイルを示す受信信号プロファイルRSSIを生成して鍵作成部160へ出力する。

**【0069】**

パターンP1～Pnによってアレーアンテナ20の指向性を複数個に順次切換えて無線装置30から無線装置10へデータを送信したとき、無線装置10のプロファイル生成部150が受信信号プロファイルRSSIを生成する。

**【0070】**

鍵作成部160は、プロファイル生成部150から受信信号プロファイルRSSIを受け、受信信号プロファイルRSSIから最大強度WImax (=WI6)を検出する。そして、鍵作成部160は、最大強度WImax (=WI6)によって受信信号プロファイルRSSIを規格化し、各強度WI1～WI nを多値化する。鍵作成部160は、多値化した各値を検出し、その検出した各値をビットパターンとする秘密鍵Ks1またはKs2を作成する。

**【0071】**

図8は、図1に示す2つの無線装置10、30間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置30の送信処理部120は、k=1を設定する(ステップS1)。そして、指向性設定部230は、パターンP1によりアレーアンテナ20の指向性を1つの指向性に設定する(ステップS2)。

**【0072】**

その後、無線装置10の信号発生部110は、所定の信号を発生して送信処理部120へ出力する。送信処理部120は、所定の信号に変調等の処理を施し、アンテナ11を介して無線装置30へ所定の信号を構成する電波を送信する(ステップS3)。

**【0073】**

無線装置30において、アレーアンテナ20は、無線装置10からの電波を受信し、その受信した電波をプロファイル生成部150へ出力する。プロファイル生成部150は、アレーアンテナ20から受けた電波の強度I1kを検出する(ステップS4)。

**【0074】**

その後、無線装置30の信号発生部110は、所定の信号を発生して送信処理部120へ出力する。送信処理部120は、所定の信号に変調等の処理を施し、アレーアンテナ20を介して無線装置10へ所定の信号を構成する電波を送信する(ステップS5)。

**【0075】**

無線装置10において、アンテナ11は、無線装置30からの電波を受信し、その受信した電波をプロファイル生成部150へ出力する。プロファイル生成部150は、アンテナ11から受けた電波の強度I2kを検出する(ステップS6)。

**【0076】**

その後、無線装置30の送信処理部120は、k=k+1を設定し(ステップS7)、k=nであるか否かを判定する(ステップS8)。そして、k=nでないとき、ステップS2～S8が繰返し実行される。即ち、アレーアンテナ20の指向性がパターンP1～Pnによってn個に変えられて、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間で所定の信号を構成する電波が送受信され、強度I11～I1n及びI21～I2nが検出されるまで、ステップS2～S8が繰返し実行される。

**【0077】**

ステップS8において、k=nであると判定されると、無線装置30において、プロファイル生成部150は、強度I11～I1nから受信信号プロファイルRSSI1を作成して鍵作成部160へ出力する。

**【0078】**

鍵作成部160は、受信信号プロファイルRSSI1から最大強度WImax1を検出し、その検出した最大強度WImax1によって受信信号プロファイルRSSI1を規格化し、強度I11～I1nを多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵Ks2を生成する(ステップS9)。

**【0079】**

また、無線装置10のプロファイル生成部150は、強度I21～I2nから受信信号プロファイルRSSI2を作成して鍵作成部160へ出力する。鍵作成部160は、受信

信号プロファイルRSSI2から最大強度 $W_{I\max 2}$ を検出し、その検出した最大強度 $W_{I\max 2}$ によって受信信号プロファイルRSSI2を規格化し、強度 $I_{21} \sim I_{2n}$ を多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵 $K_{s1}$ を生成する(ステップS10)。

【0080】

その後、無線装置10において、鍵作成部160は、秘密鍵 $K_{s1}$ を鍵一致確認部170へ出力する。鍵一致確認部170のデータ発生部171は、上述した方法によって鍵確認用データDCFM1を発生して送信処理部120及びデータ比較部172へ出力する。送信処理部120は、鍵確認用データDCFM1に変調等の処理を施し、アンテナ部130を介して無線装置30へ鍵確認用データDCFM1を送信する。

【0081】

そして、アンテナ部130は、無線装置30において発生された鍵確認用データDCFM2を無線装置30から受信し、その受信した鍵確認用データDCFM2を受信処理部140へ出力する。受信処理部140は、鍵確認用データDCFM2に所定の処理を施し、鍵一致確認部170のデータ比較部172へ鍵確認用データDCFM2を出力する。

【0082】

データ比較部172は、データ発生部171からの鍵確認用データDCFM1を受信処理部140からの鍵確認用データDCFM2と比較する。そして、データ比較部172は、鍵確認用データDCFM1が鍵確認用データDCFM2に一致しているとき、一致信号MTHを生成して結果処理部173へ出力する。結果処理部173は、一致信号MTHに応じて、鍵作成部160からの秘密鍵 $K_{s1}$ を鍵記憶部180に記憶する。

【0083】

一方、鍵確認用データDCFM1が鍵確認用データDCFM2に不一致であるとき、データ比較部172は、不一致信号NMTHを生成して送信処理部120及び鍵一致化部190へ出力する。送信処理部120は、不一致信号NMTHをアンテナ部130を介して無線装置30へ送信する。そして、無線装置30は、無線装置10において秘密鍵 $K_{s1}$ 、 $K_{s2}$ の不一致が確認されたことを検知する。

【0084】

これにより、無線装置10における鍵一致の確認が終了する(ステップS11)。

【0085】

無線装置30においても、無線装置10と同じ動作によって鍵一致の確認が行なわれる(ステップS12)。

【0086】

ステップS11において、秘密鍵 $K_{s1}$ 、 $K_{s2}$ の不一致が確認されたとき、無線装置10において、鍵一致化部190の擬似シンドローム作成部191は、鍵一致確認部170から不一致信号NMTHを受ける。そして、擬似シンドローム作成部191は、不一致信号NMTHに応じて、鍵作成部160から受けた秘密鍵 $K_{s1}$ のビットパターン $x_1$ を検出し、その検出したビットパターン $x_1$ のシンドローム $s_1 = x_1 H^T$ を演算する。

【0087】

擬似シンドローム作成部191は、演算したシンドローム $s_1 = x_1 H^T$ を不一致ビット検出部192へ出力し、ビットパターン $x_1$ を鍵不一致訂正部193へ出力する。

【0088】

一方、無線装置30は、ステップS11において無線装置10から不一致信号NMTHを受信し、その受信した不一致信号NMTHに応じて、シンドローム $s_2 = x_2 H^T$ を演算して無線装置10へ送信する。

【0089】

無線装置10のアンテナ部130は、無線装置30からシンドローム $s_2 = x_2 H^T$ を受信して受信処理部140へ出力する。受信処理部140は、シンドローム $s_2 = x_2 H^T$ に対して所定の処理を施し、シンドローム $s_2 = x_2 H^T$ を鍵一致化部190へ出力する。

## 【0090】

鍵一致化部190の不一致ビット検出部192は、受信処理部140から無線装置30において作成されたシンドローム  $s_2 = x_2 H^T$  を受ける。そして、不一致ビット検出部192は、無線装置10で作成されたシンドローム  $s_1 = x_1 H^T$  と無線装置30において作成されたシンドローム  $s_2 = x_2 H^T$  との差分  $s = s_1 - s_2$  を演算する。

## 【0091】

その後、不一致ビット検出部192は、 $s \neq 0$ であることを確認し、鍵不一致のビットパターン  $e = x_1 - x_2$  を  $s = e H^T$  に基づいて演算し、その演算した鍵不一致のビットパターン  $e$  を鍵不一致訂正部193へ出力する。

## 【0092】

鍵不一致訂正部193は、擬似シンドローム作成部191からのビットパターン  $x_1$  と、不一致ビット検出部192からの鍵不一致のビットパターン  $e$  とに基づいて、無線装置30において作成された秘密鍵  $K_{s2}$  のビットパターン  $x_2 = x_1 - e$  を演算する。

## 【0093】

そして、データ発生部194、データ比較部195及び結果処理部196は、鍵一致確認部170における鍵一致確認の動作と同じ動作によって、一致化された鍵  $x_2 = x_1 - e$  の一致を確認する。

## 【0094】

これにより、鍵不一致対策が終了する（ステップS13）。

## 【0095】

無線装置30においても、無線装置10と同じ動作によって鍵不一致対策が行なわれる（ステップS14）。

## 【0096】

ステップS11において、秘密鍵  $K_{s1}$  が秘密鍵  $K_{s2}$  に一致することが確認されたとき、またはステップS13において鍵不一致対策がなされたとき、暗号部200は、鍵記憶部180から秘密鍵  $K_{s1}$  を読出して送信データを暗号化し、暗号化した送信データを送信処理部120へ出力する。そして、送信処理部120は、暗号化された送信データに変調等を施し、アンテナ部130を介して暗号化された送信データを無線装置30へ送信する。

## 【0097】

また、アンテナ部130は、暗号化された送信データを無線装置30から受信し、その受信した暗号化された送信データを受信処理部140へ出力する。受信処理部140は、暗号化された送信データに所定の処理を施し、暗号化された送信データを復号部210へ出力する。

## 【0098】

復号部210は、受信処理部140からの暗号化された送信データを復号して受信データを取得する。

## 【0099】

これにより、秘密鍵  $K_{s1}$  による暗号・復号が終了する（ステップS15）。

## 【0100】

無線装置30においても、無線装置10と同じ動作によって秘密鍵  $K_{s2}$  による暗号・復号が行なわれる（ステップS16）。そして、一連の動作が終了する。

## 【0101】

上述したステップS3、S4に示す動作は、無線装置30において受信信号プロファイルRSSI1を生成するための電波を無線装置10のアンテナ11から無線装置30のアレーアンテナ20へ送信し、かつ、無線装置30において電波の強度I1kを検出する動作であり、ステップS5、S6に示す動作は、無線装置10において受信信号プロファイルRSSI2を生成するための電波を無線装置30のアレーアンテナ20から無線装置10のアンテナ11へ送信し、かつ、無線装置10において電波の強度I2kを検出する動作である。そして、所定の信号を構成する電波の無線装置10のアンテナ11から無線装

置 30 のアレーアンテナ 20 への送信及び所定の信号を構成する電波の無線装置 30 のアレーアンテナ 20 から無線装置 10 のアンテナ 11 への送信は、アレーアンテナ 20 の指向性を 1 つの指向性に設定して交互に行なわれる。つまり、所定の信号を構成する電波は、無線装置 10 のアンテナ 11 と無線装置 30 のアレーアンテナ 20 との間で時分割復信 (TDD) により送受信される。

#### 【0102】

従って、アレーアンテナ 20 の指向性を 1 つの指向性に設定して無線装置 10 のアンテナ 11 から無線装置 30 のアレーアンテナ 20 へ所定の信号を構成する電波を送信し、無線装置 30 において電波の強度  $I_{1k}$  を検出した直後に、同じ所定の信号を構成する電波を無線装置 30 のアレーアンテナ 20 から無線装置 10 のアンテナ 11 へ送信し、無線装置 10 において電波の強度  $I_{2k}$  を検出することができる。その結果、無線装置 10、30 間において同じ伝送路特性を確保して所定の信号を構成する電波を無線装置 10、30 間で送受信でき、電波の可逆性により電波の強度  $I_{11} \sim I_{1n}$  をそれぞれ電波の強度  $I_{21} \sim I_{2n}$  に一致させることができる。そして、無線装置 10 において作成される秘密鍵  $K_{s1}$  を無線装置 30 において作成される秘密鍵  $K_{s2}$  に容易に一致させることができる。

#### 【0103】

また、所定の信号を構成する電波は、無線装置 10、30 間で時分割復信 (TDD) により送受信されるので、電波の干渉を抑制して 1 つのアレーアンテナ 20 を介して所定の信号を構成する電波を無線装置 10、30 間で送受信できる。

#### 【0104】

更に、アレーアンテナ 20 の指向性を 1 つの指向性に設定して無線装置 10、30 間で所定の信号を構成する電波を送受信し、秘密鍵  $K_{s1}$ 、 $K_{s2}$  を作成するための受信信号プロファイル  $RSSI_1$ 、 $RSSI_2$  を生成するので、図 1 に示すようにアレーアンテナ 20 を装着した無線装置 30 の近傍に盗聴装置 50 が配置されていても、盗聴装置 50 による秘密鍵  $K_{s1}$ 、 $K_{s2}$  の盗聴を抑制できる。

#### 【0105】

即ち、盗聴装置 50 は、アンテナ 11 及びアレーアンテナ 20 から送信された電波をアンテナ 51 を介して受信するが、アレーアンテナ 20 は指向性を各指向性に設定して電波を送受信するので、アンテナ 11 とアレーアンテナ 20 との間で送受信される電波は、アンテナ 11 またはアレーアンテナ 20 とアンテナ 51 との間で送受信される電波と異なり、盗聴装置 50 は、無線装置 30 が送受信する電波と同じ電波を送受信できず、電波の強度  $I_{1k}$  と同じ強度を得ることができない。その結果、盗聴装置 50 は、秘密鍵  $K_{s1}$ 、 $K_{s2}$  を盗聴することができない。

#### 【0106】

従って、この発明においては、電氣的に指向性を切換え可能なアレーアンテナ 20 を盗聴装置 50 の近傍に配置された無線装置 30 に装着することを特徴とする。

#### 【0107】

更に、鍵確認用データ  $DCFM_1 \sim 4$  は、秘密鍵  $K_{s1}$ 、 $K_{s2}$  に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データ  $DCFM_1 \sim 4$  が盗聴されても秘密鍵  $K_{s1}$ 、 $K_{s2}$  が解読される危険性を極めて低くできる。

#### 【0108】

更に、シンδροーム  $s_1$ 、 $s_2$  は、秘密鍵  $K_{s1}$ 、 $K_{s2}$  のビットパターンを示す鍵  $x_1$ 、 $x_2$  に検査行列  $H$  の転置行列  $H^T$  を乗算して得られるので、シンδροーム  $s_1$ 、 $s_2$  が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

#### 【0109】

なお、無線装置 10、30 間で通信を行なう動作は、実際には、CPU (Central Processing Unit) によって行なわれ、無線装置 10 に搭載された CPU は、図 8 に示す各ステップ  $S_3$ 、 $S_6$ 、 $S_{10}$ 、 $S_{11}$ 、 $S_{13}$ 、 $S_{15}$  を備えるプ

プログラムをROM (Read Only Memory) から読出し、無線装置30に搭載されたCPUは、図8に示す各ステップS1, S2, S4, S5, S7, S8, S9, S12, S14, S16を備えるプログラムをROMから読出し、無線装置10, 30に搭載された2つのCPUは、その読出したプログラムを実行して図8に示すフローチャートに従って無線装置10, 30間で通信を行なう。

【0110】

従って、ROMは、無線装置10, 30間で通信を行なう動作をコンピュータ (CPU) に実行させるためのプログラムを記録したコンピュータ (CPU) 読取り可能な記録媒体に相当する。

【0111】

そして、図8に示す各ステップを備えるプログラムは、アレーアンテナ20の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置10, 30間における通信をコンピュータ (CPU) に実行させるプログラムである。

【0112】

上記においては、電気的に指向性を切換え可能なアレーアンテナ20を無線装置30のみに装着すると説明したが、この発明においては、アレーアンテナ20は、無線装置10及び30の両方に装着されてもよい。

【0113】

即ち、この発明においては、アレーアンテナ20は、2つの無線装置10, 30のうち、少なくとも一方の無線装置に装着されていればよい。そして、アレーアンテナ20を装着した無線装置は、好ましくは、盗聴装置50の近傍に配置される。

【0114】

また、この発明においては、秘密鍵Ks1, Ks2の鍵長は、無線装置10, 30間の通信環境に応じて決定されてもよい。即ち、無線装置10, 30間の通信環境が盗聴し易い環境であるとき、秘密鍵Ks1, Ks2の鍵長を相対的に長くし、無線装置10, 30間の通信環境が盗聴しにくい環境であるとき、秘密鍵Ks1, Ks2の鍵長を相対的に短くする。

【0115】

更に、定期的に秘密鍵Ks1, Ks2の鍵長を変えるようにしてもよい。

【0116】

更に、無線装置10, 30間で送受信する情報の機密性に応じて秘密鍵Ks1, Ks2の鍵長を変えるようにしてもよい。即ち、情報の機密性が高いとき秘密鍵Ks1, Ks2の鍵長を相対的に長くし、情報の機密性が低いとき秘密鍵Ks1, Ks2の鍵長を相対的に短くする。

【0117】

そして、この鍵長は、アレーアンテナ20の指向性を変化させる個数、即ち、制御電圧CLV1~CLVnの個数により制御される。秘密鍵Ks1, Ks2は、検出された電波の強度I11~I1n, I21~I2nの個数からなるビットパターンを有し、電波の強度I11~I1n, I21~I2nの個数は、アレーアンテナ20の指向性を変化させる個数に等しいからである。つまり、制御電圧CLV1~CLVnの個数により秘密鍵Ks1, Ks2の鍵長を制御できる。

【0118】

このように、この発明においては、秘密鍵Ks1, Ks2の鍵長は、電気的に指向性を切換え可能なアレーアンテナ20の指向性を変化させる個数によって決定される。

【0119】

更に、上記においては、2つの無線装置間において秘密鍵を生成する場合、即ち、1つの無線装置が1つの無線装置と通信する場合について説明したが、この発明は、これに限らず、1つの無線装置が複数の無線装置と通信する場合についても適用される。この場合、1つの無線装置は、通信の相手毎にアレーアンテナ20の指向性の切換パターンを変えて秘密鍵を生成する。1つの無線装置は、アレーアンテナ20の指向性の切換パターンを



1つに固定して複数の無線装置との間で秘密鍵を生成することも可能であるが（複数の無線装置の設置場所によって1つの無線装置との伝送路が異なるので、通信の相手毎に異なる秘密鍵を生成できる）、盗聴を効果的に抑制するには、通信の相手毎にアレーアンテナ20の指向性の切換パターンを変えて秘密鍵を生成するのが好ましい。

#### 【0120】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

#### 【産業上の利用可能性】

#### 【0121】

この発明は、秘密鍵の盗聴を抑制可能な無線通信システムに適用される。

#### 【図面の簡単な説明】

#### 【0122】

【図1】 この発明の実施の形態による無線通信システムの概略図である。

【図2】 図1に示す一方の無線装置の概略ブロック図である。

【図3】 図1に示す他方の無線装置の概略ブロック図である。

【図4】 図3に示す指向性設定部の概略ブロック図である。

【図5】 図2及び図3に示す鍵一致確認部の概略ブロック図である。

【図6】 図2及び図3に示す鍵一致化部の概略ブロック図である。

【図7】 受信信号プロファイルRSSIの概念図である。

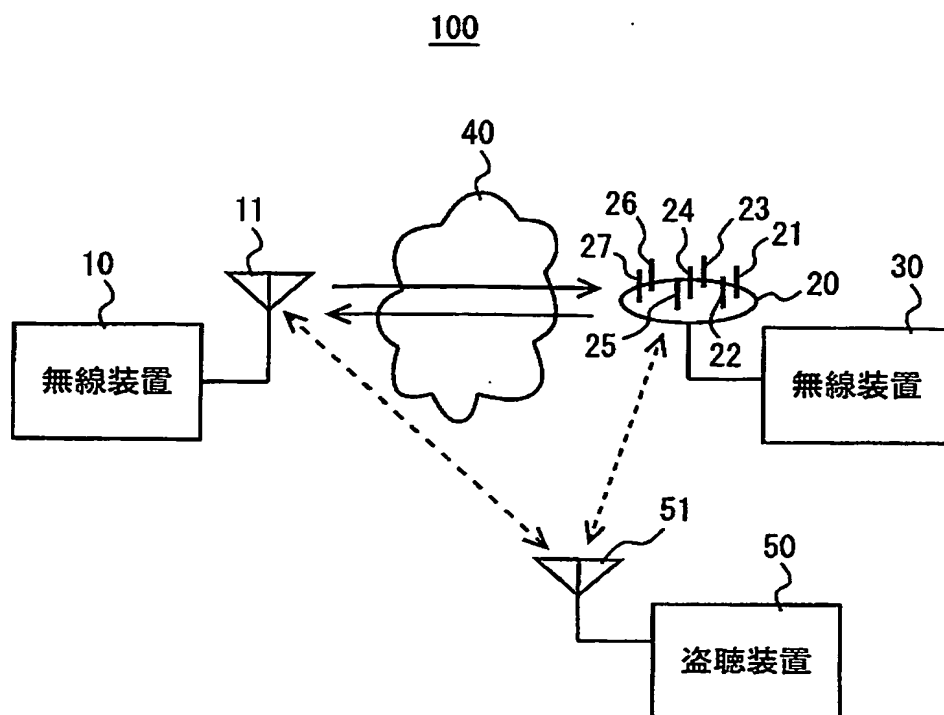
【図8】 図1に示す2つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

#### 【符号の説明】

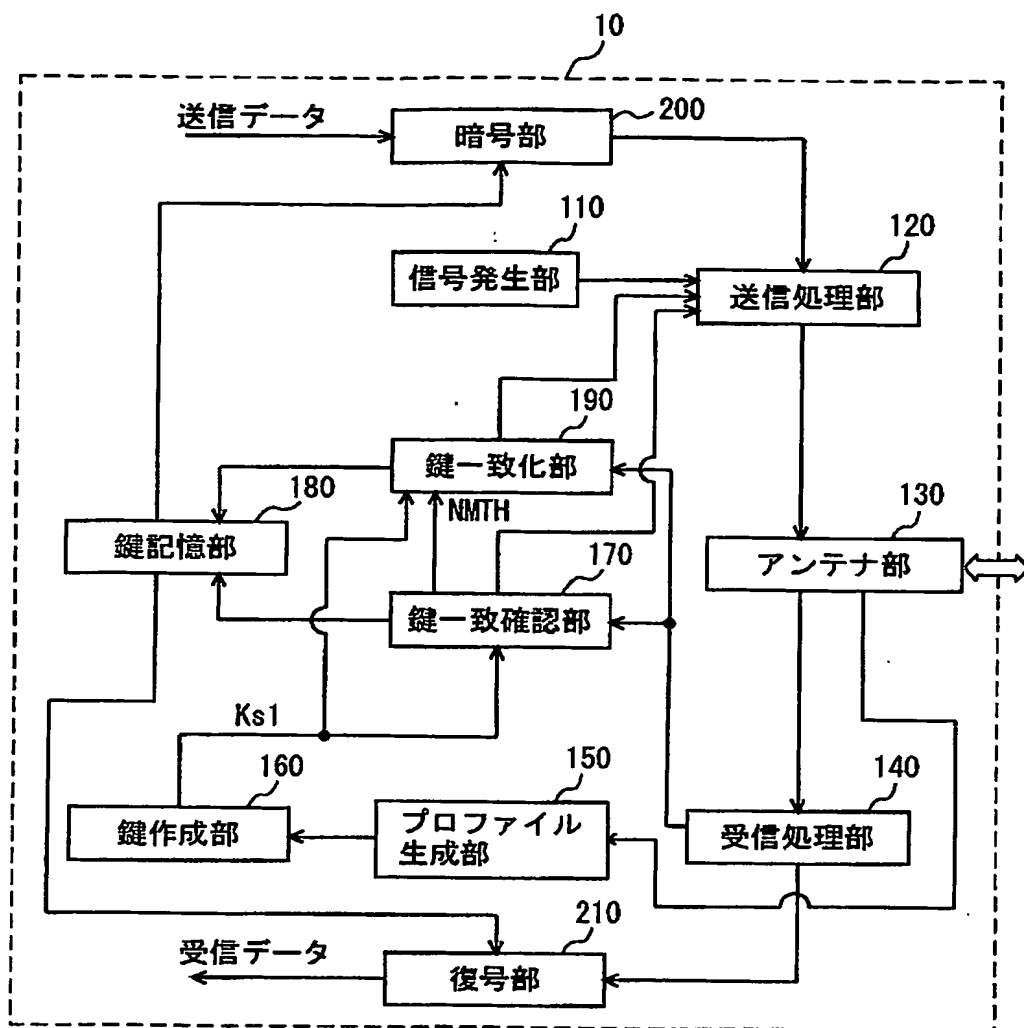
#### 【0123】

10, 30 無線装置、11, 51 アンテナ、20 アレーアンテナ、21～27  
アンテナ素子、40 中間物、50 盗聴装置、100 無線通信システム、110 信号発生部、120 送信処理部、130, 220 アンテナ部、140 受信処理部、150  
プロファイル生成部、160 鍵作成部、170 鍵一致確認部、171, 194  
データ発生部、172, 195 データ比較部、173, 196 結果処理部、180  
鍵記憶部、190 鍵一致化部、191 擬似シンドローム作成部、192 不一致ビット検出部、193 鍵不一致訂正部、200 暗号部、210 復号部、230 指向性設定部、231 制御電圧発生回路、232 バラクタダイオード。

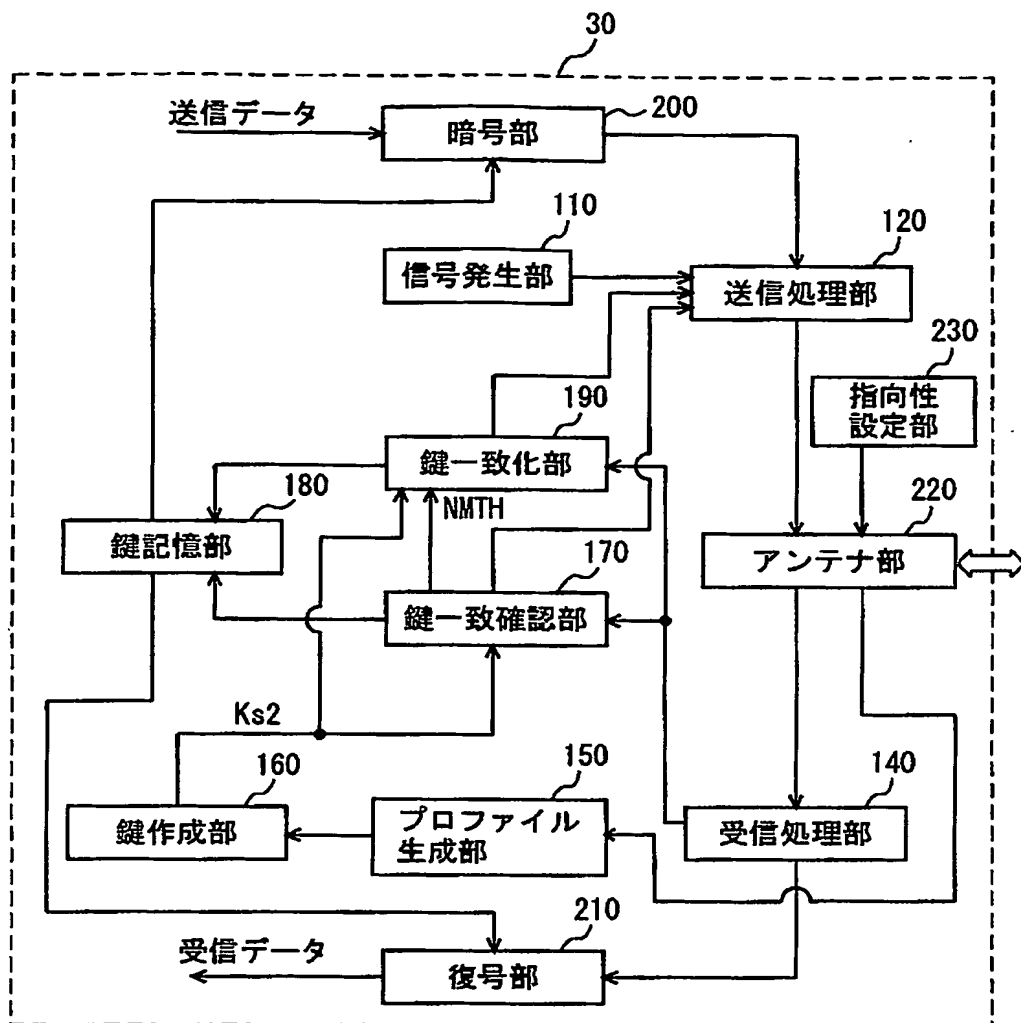
【書類名】 図面  
【図 1】



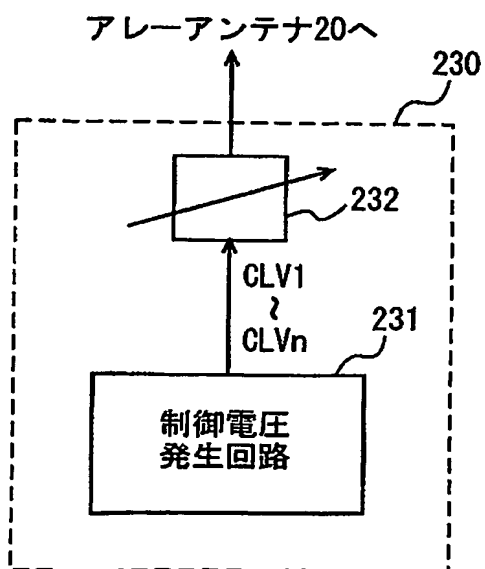
【図 2】



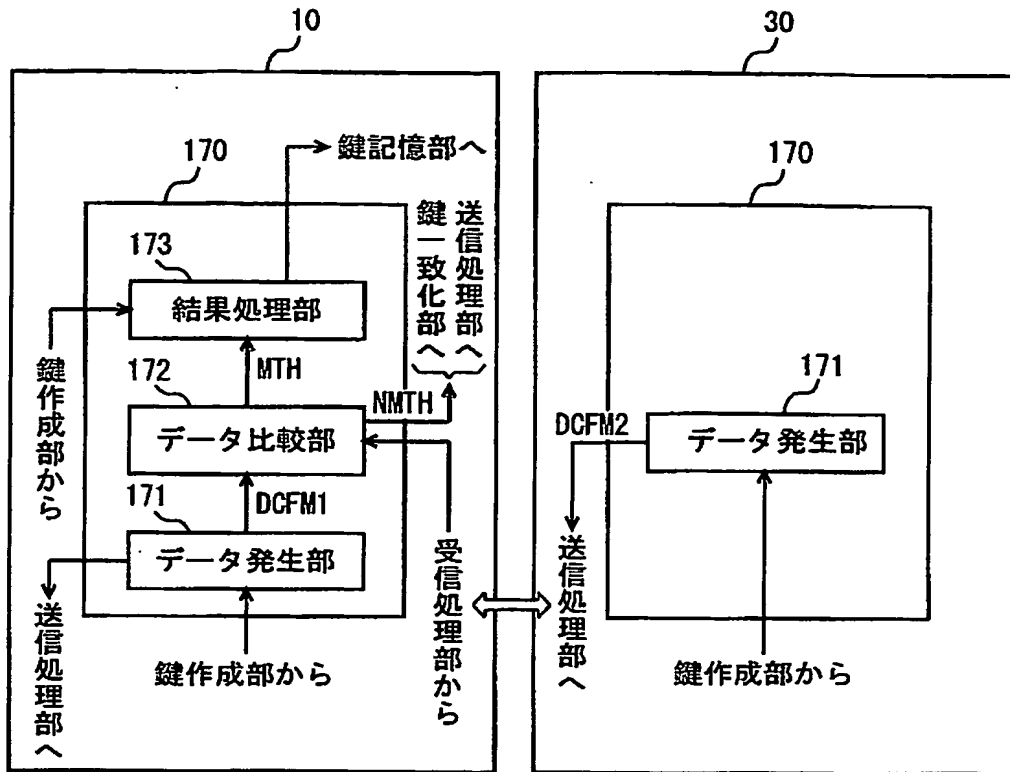
【図 3】



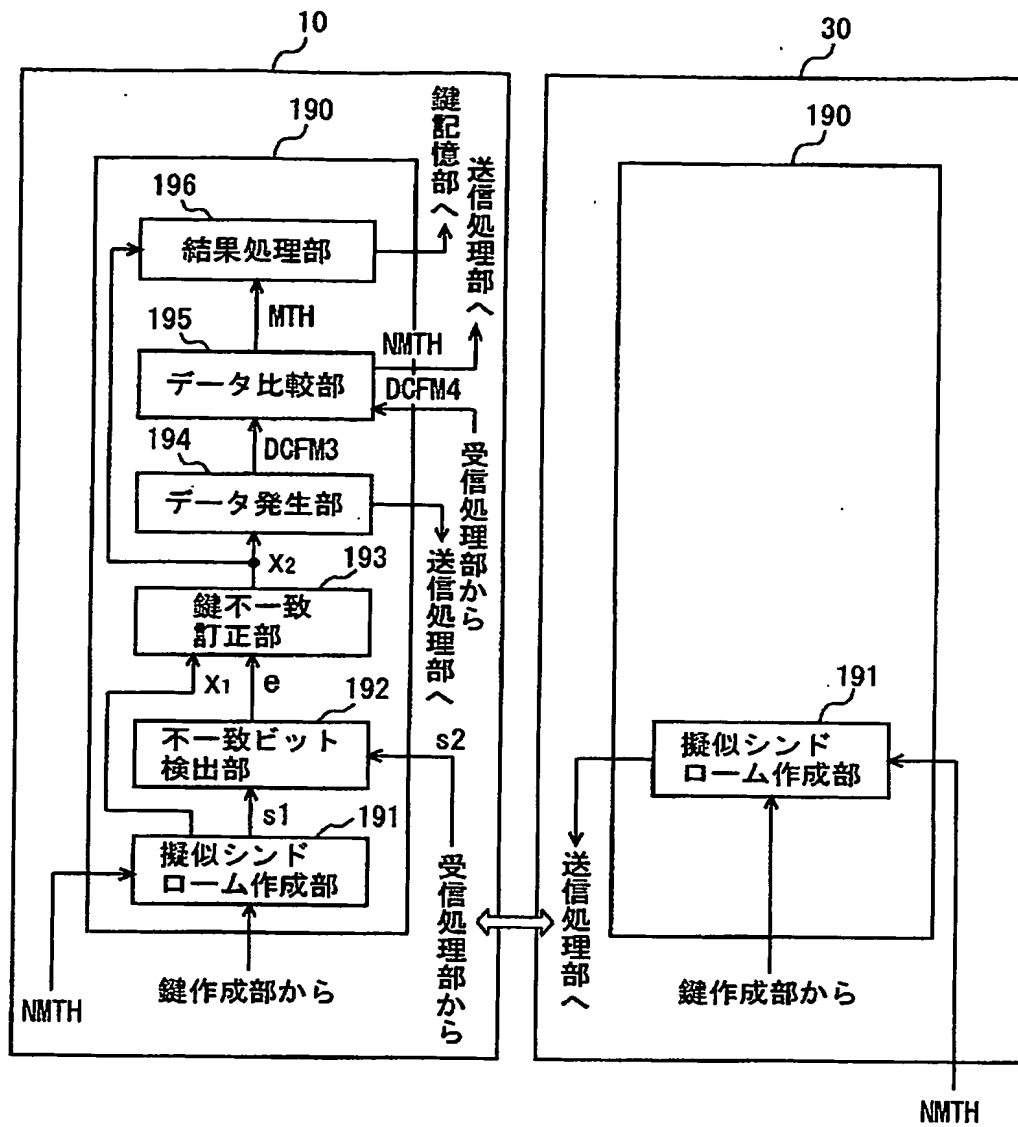
【図 4】



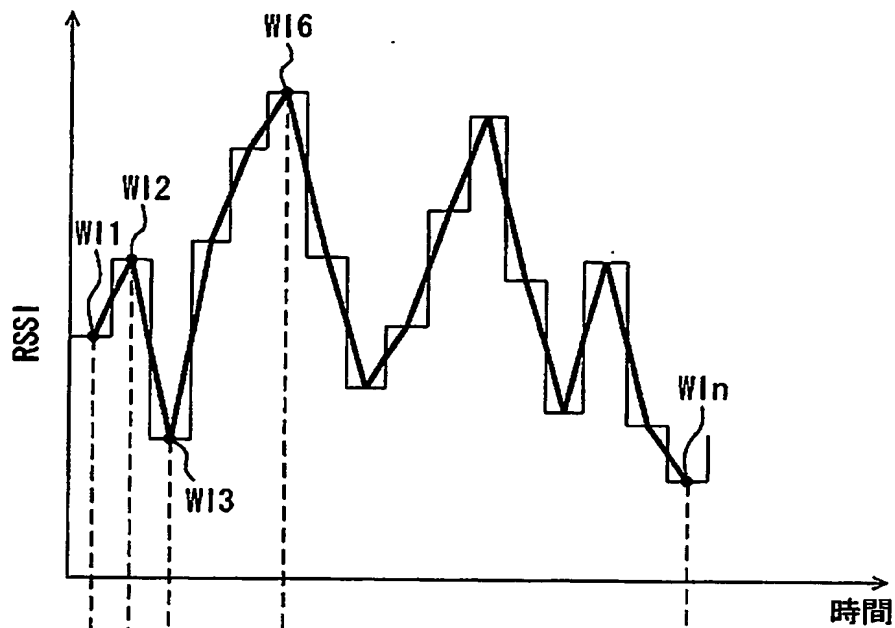
【図 5】



【図 6】

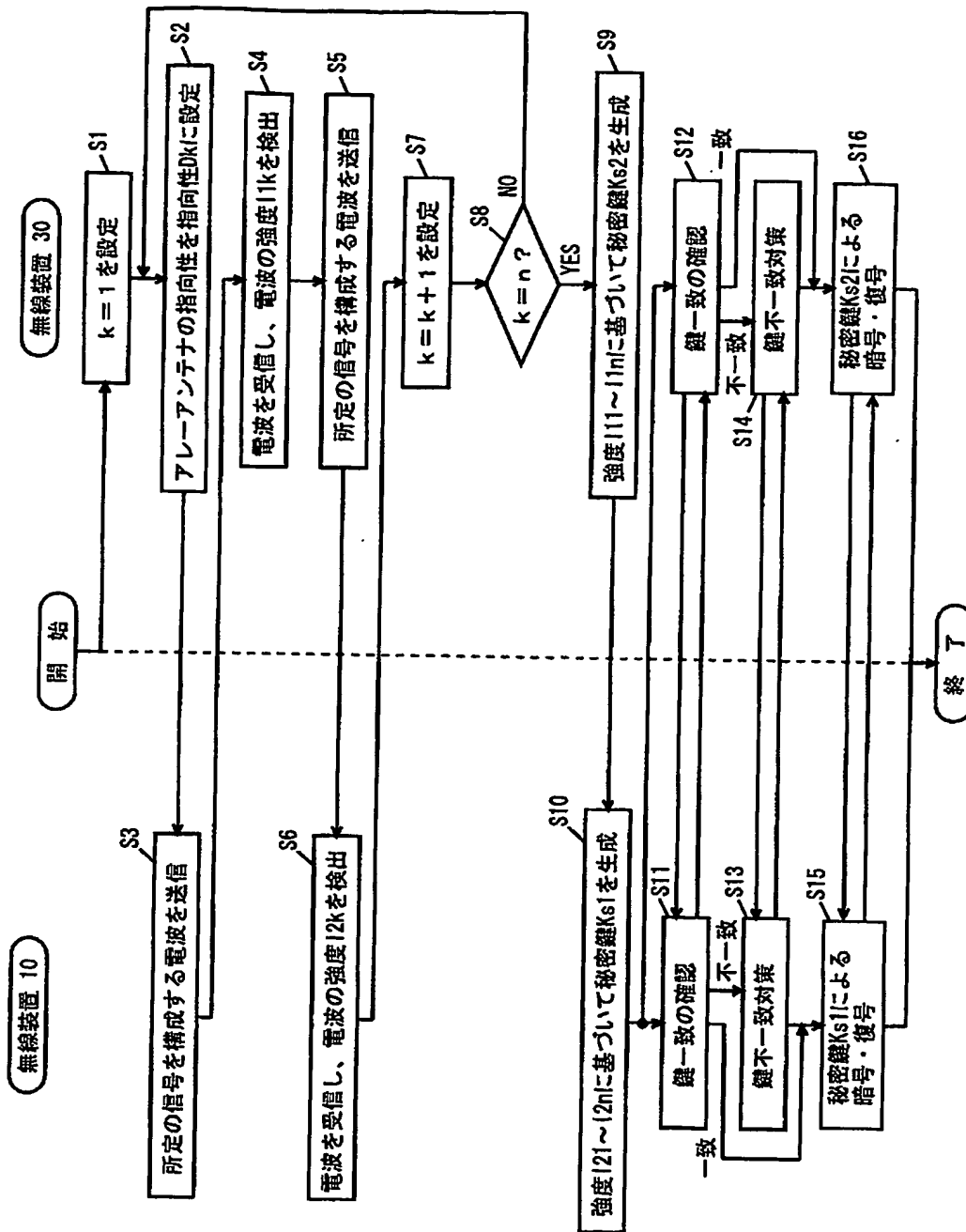


【図 7】



	P1	P2	P3	..	P6	.....	Pn
V1	0	1	2		0		0
V2	0	0	0		1		1
V3	1	0	0		0		0
V4	0	0	0	..	0	.....	2
V5	0	0	0		0		0
V6	0	0	0		0		1

【図8】





## 【書類名】 要約書

## 【要約】

【課題】 秘密鍵の盗聴を抑制可能な無線通信システムを提供する。

【解決手段】 無線通信システム 100 は、無線装置 10、30 と、アンテナ 11 と、アレーアンテナ 20 とを備える。無線装置 10 及び 30 は、アレーアンテナ 20 の指向性を複数個に変えながら時分割復信 (TDD) により所定の信号をアンテナ 11 及びアレーアンテナ 20 を介して相互に送受信する。そして、無線装置 10 及び 30 は、受信した複数の電波の強度を検出して複数の強度のプロファイルを示す受信信号プロファイル RSSI 1, 2 をそれぞれ作成する。無線装置 10 及び 30 は、それぞれ、受信信号プロファイル RSSI 1, 2 の複数の強度を多値化し、その多値化した複数の値をビットパターンとする秘密鍵 Ks 1, Ks 2 を作成する。

【選択図】 図 1

特願 2003-312156

出 願 人 履 歴 情 報

識別番号 [503027931]

1. 変更年月日 2003年 4月 4日

[変更理由] 住所変更

住 所 京都府京都市上京区今出川通烏丸東入玄武町601  
氏 名 学校法人同志社

特願 2 0 0 3 - 3 1 2 1 5 6

出 願 人 履 歴 情 報

識別番号 [ 3 9 3 0 3 1 5 8 6 ]

1. 変更年月日	2 0 0 0 年 3 月 2 7 日
[変更理由]	住所変更
住 所	京都府相楽郡精華町光台二丁目 2 番地 2
氏 名	株式会社国際電気通信基礎技術研究所

PCT/JP2004/002228

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

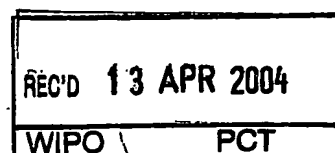
25.2.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2004年 1月 5日

出 願 番 号  
Application Number: 特願2004-000533  
[ST. 10/C]: [J.P.2004-000533]



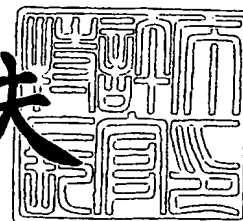
出 願 人  
Applicant(s): 学校法人同志社  
株式会社国際電気通信基礎技術研究所

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 3月26日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2004-3025117

【書類名】 特許願  
【整理番号】 1032333  
【提出日】 平成16年 1月 5日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04B 13/00  
【発明者】  
    【住所又は居所】 京都府京田辺市多々羅都谷 1-3 同志社大学内  
    【氏名】 笹岡 秀一  
【発明者】  
    【住所又は居所】 京都府相楽郡精華町光台二丁目 2 番地 2 株式会社国際電気通信  
    基礎技術研究所内  
    【氏名】 青野 智之  
【発明者】  
    【住所又は居所】 京都府相楽郡精華町光台二丁目 2 番地 2 株式会社国際電気通信  
    基礎技術研究所内  
    【氏名】 大平 孝  
【特許出願人】  
    【識別番号】 503027931  
    【住所又は居所】 京都府京都市上京区今出川通烏丸東入玄武町 6 0 1 番地  
    【氏名又は名称】 学校法人同志社  
【特許出願人】  
    【識別番号】 393031586  
    【住所又は居所】 京都府相楽郡精華町光台二丁目 2 番地 2  
    【氏名又は名称】 株式会社国際電気通信基礎技術研究所  
【代理人】  
    【識別番号】 100064746  
    【弁理士】  
    【氏名又は名称】 深見 久郎  
【選任した代理人】  
    【識別番号】 100085132  
    【弁理士】  
    【氏名又は名称】 森田 俊雄  
【選任した代理人】  
    【識別番号】 100083703  
    【弁理士】  
    【氏名又は名称】 仲村 義平  
【選任した代理人】  
    【識別番号】 100096781  
    【弁理士】  
    【氏名又は名称】 堀井 豊  
【選任した代理人】  
    【識別番号】 100098316  
    【弁理士】  
    【氏名又は名称】 野田 久登  
【選任した代理人】  
    【識別番号】 100109162  
    【弁理士】  
    【氏名又は名称】 酒井 将行

【国等の委託研究の成果に係る記載事項】 平成15年度通信・放送機構、研究テーマ「自律分散型無線ネットワークの研究開発」に関する委託研究、産

業活力再生特別措置法第 3 0 条の適用を受ける特許出願

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 特許請求の範囲 1

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0315129

【包括委任状番号】 0005582

**【書類名】 特許請求の範囲****【請求項 1】**

指向性を電氣的に切換え可能な第 1 のアンテナと、  
第 2 のアンテナと、

前記第 1 及び第 2 のアンテナを介して無線伝送路により電波を相互に送受信する第 1 及び第 2 の無線装置とを備え、

前記第 1 の無線装置は、前記第 1 のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第 2 の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第 1 の受信信号プロファイルを生成し、その生成した第 1 の受信信号プロファイルに基づいて第 1 の秘密鍵を生成し、

前記第 2 の無線装置は、前記第 1 のアンテナの指向性が所定のパターンにより複数個に変えられたときに前記第 1 の無線装置が前記所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第 2 の受信信号プロファイルを生成し、その生成した第 2 の受信信号プロファイルに基づいて前記第 1 の秘密鍵と同じ第 2 の秘密鍵を生成する、無線通信システム。

**【請求項 2】**

前記第 1 の無線装置は、前記第 1 のアンテナが無指向性に制御されたときに前記第 2 の無線装置との間で前記無線伝送路を確立し、前記無線伝送路が確立した後、前記第 1 のアンテナの指向性を前記複数個に変えながら前記第 2 の無線装置との間で前記複数のデータを送受信する、請求項 1 に記載の無線通信システム。

**【請求項 3】**

前記第 1 の無線装置は、前記第 2 の無線装置との間における前記各データの送受信において、前記第 1 のアンテナの指向性を更新して前記第 2 の無線装置から前記データを受信し、前記更新した前記第 1 のアンテナの指向性を維持して前記受信したデータを前記第 2 の無線装置へ送信する、請求項 2 に記載の無線通信システム。

**【請求項 4】**

前記所定の通信プロトコルは、複数の階層からなり、

前記複数のデータは、前記複数の階層のうち、前記データを前記電気信号に変換する階層におけるデータフォーマットに含まれ、

前記データを前記電気信号に変換する階層は、複数の通信プロトコルに共通な階層である、請求項 2 または請求項 3 に記載の無線通信システム。

**【請求項 5】**

前記複数のデータの各々は、前記第 1 および第 2 の無線装置により受信された電波の強度を検出する区間と、前記第 1 のアンテナの指向性を変更する区間とからなる、請求項 1 から請求項 4 のいずれか 1 項に記載の無線通信システム。

**【請求項 6】**

前記第 1 の無線装置は、前記生成した第 1 の秘密鍵が前記第 2 の秘密鍵に不一致であるとき、前記第 1 の秘密鍵を前記第 2 の秘密鍵に一致させる、請求項 1 から請求項 5 のいずれか 1 項に記載の無線通信システム。

**【請求項 7】**

前記第 1 のアンテナは、盗聴者の端末に近接して配置された第 1 の無線装置に設置される、請求項 1 から請求項 6 のいずれか 1 項に記載の無線通信システム。

**【請求項 8】**

前記第 1 及び第 2 の無線装置は、前記第 1 及び第 2 の秘密鍵を用いてデータを暗号及び復号して相互に通信する、請求項 1 から請求項 7 のいずれか 1 項に記載の無線通信システム。

【書類名】明細書

【発明の名称】無線通信システム

【技術分野】

【0001】

この発明は、無線通信システムに関し、特に、暗号化した情報を無線により通信する無線通信システムに関するものである。

【背景技術】

【0002】

最近、情報化社会の発展に伴い情報通信が益々重要になるとともに、情報の盗聴または不正利用がより深刻な問題となっている。このような情報の盗聴を防止するために従来から情報を暗号化して送信することが行なわれている。

【0003】

情報を暗号化して端末間で通信を行なう方式として公開鍵暗号方式と秘密鍵暗号方式とがある。公開鍵暗号方式は、安全性は高いが、大容量のデータの暗号化には向かない。

【0004】

一方、秘密鍵暗号方式は、処理が比較的簡単であり、大容量のデータの高速暗号化も可能であるが、秘密鍵を通信の相手方に送信する必要がある。また、秘密鍵暗号方式は、同一の秘密鍵を使用し続けると、暗号解読の攻撃を受けやすく、安全性が損なわれる可能性がある。

【0005】

そこで、秘密鍵を相手方に送信せずに秘密鍵を共有する方法として、2つの端末間の伝送路の特性を測定し、その測定した特性に基づいて各端末で秘密鍵を生成する方法が提案されている（非特許文献1）。

【0006】

この方法は、2つの端末間でデータを送受信したときの遅延プロファイルを各端末で測定し、その測定した遅延プロファイルをアナログ信号からデジタル信号に変換して各端末で秘密鍵を生成する方法である。即ち、伝送路を伝搬する電波は可逆性を示すために、一方の端末から他方の端末へデータを送信したときの遅延プロファイルは、他方の端末から一方の端末へ同じデータを送信したときの遅延プロファイルと同じになる。従って、一方の端末で測定した遅延プロファイルに基づいて生成された秘密鍵は、他方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵と同じになる。

【0007】

このように、伝送路特性を用いて秘密鍵を生成する方法は、同じデータを2つの端末間で相互に送信するだけで同じ秘密鍵を共有することができる。

【非特許文献1】堀池 元樹、笹岡 秀一、「陸上移動通信路の不規則変動に基づく秘密鍵共有方式」、信学技報、社団法人 電子情報通信学会、2002年10月、TECHNICAL REPORT OF IEICE RCS2002-173, p. 7-12

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかし、2つの端末間で送信されるデータを盗聴者が各端末の近傍で傍受して遅延プロファイルを測定すれば、盗聴者は、各端末で測定した遅延プロファイルに近い遅延プロファイルを取得することができる。その結果、秘密鍵が解読される可能性がある。

【0009】

そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、秘密鍵の盗聴を抑制することができる無線通信システムを提供することである。

【課題を解決するための手段】

【0010】

この発明によれば、無線通信システムは、第1および第2のアンテナと、第1および第2の無線装置とを備える。第1のアンテナは、指向性を電氣的に切換え可能なアンテナで



ある。第1および第2の無線装置は、第1及び第2のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第1の無線装置は、第1のアンテナの指向性が所定のパターンにより複数個に変えられたときに第2の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第1の受信信号プロファイルを生成し、その生成した第1の受信信号プロファイルに基づいて第1の秘密鍵を生成する。また、第2の無線装置は、第1のアンテナの指向性が所定のパターンにより複数個に変えられたときに第1の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第2の受信信号プロファイルを生成し、その生成した第2の受信信号プロファイルに基づいて第1の秘密鍵と同じ第2の秘密鍵を生成する。

【0011】

好ましくは、第1の無線装置は、第1のアンテナが無指向性に制御されたときに第2の無線装置との間で無線伝送路を確立し、無線伝送路が確立した後、第1のアンテナの指向性を複数個に変えながら第2の無線装置との間で複数のデータを送受信する。

【0012】

好ましくは、第1の無線装置は、第2の無線装置との間における各データの送受信において、第1のアンテナの指向性を更新して第2の無線装置からデータを受信し、更新した第1のアンテナの指向性を維持して受信したデータを第2の無線装置へ送信する。

【0013】

好ましくは、所定の通信プロトコルは、複数の階層からなる。複数のデータは、複数の階層のうち、データを電気信号に変換する階層におけるデータフォーマットに含まれる。そして、データを電気信号に変換する階層は、複数の通信プロトコルに共通な階層である。

【0014】

好ましくは、複数のデータの各々は、第1および第2の無線装置により受信された電波の強度を検出する区間と、第1のアンテナの指向性を変更する区間とからなる。

【0015】

好ましくは、第1の無線装置は、生成した第1の秘密鍵が第2の秘密鍵に不一致であるとき、第1の秘密鍵を第2の秘密鍵に一致させる。

【0016】

好ましくは、第1のアンテナは、盗聴者の端末に近接して配置された第1の無線装置に設置される。

【0017】

好ましくは、第1及び第2の無線装置は、第1及び第2の秘密鍵を用いてデータを暗号及び復号して相互に通信する。

【発明の効果】

【0018】

この発明による無線通信システムにおいては、指向性を電氣的に切換え可能なアンテナを介して2つの無線装置間で所定のデータが所定の通信プロトコルに従って送受信される。そして、このアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが2つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて2つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、2つの無線装置間に形成される伝送路に固有である。即ち、2つの無線装置間で送受信される複数の電波を傍受して受信信号プロファイルを生成しても、その生成した受信信号プロファイルは、2つの端末装置で生成される受信信号プロファイルと異なる。

【0019】

従って、この発明によれば、2つの無線装置において作成される秘密鍵の盗聴を抑制できる。また、2つの無線装置において作成される秘密鍵を生成するためのデータを所定の

通信プロトコルに従って送受信できる。

【発明を実施するための最良の形態】

【0020】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0021】

図1は、この発明の実施の形態による無線通信システムの概略図である。無線通信システム100は、無線装置10、30と、アンテナ11と、アレーアンテナ20とを備える。無線装置10は、例えば、ユーザの移動体通信端末である。また、無線装置30は、例えば、無線アクセスポイントである。そして、無線装置10は、無線LAN (Local Area Network) のプロトコルであるIEEE802.11bまたはIEEE802.11gに従って無線装置30との間で通信を行なう。

【0022】

アンテナ11は、無線装置10に装着される。そして、アンテナ11は、全方位性のアンテナである。アレーアンテナ20は、アンテナ素子21~27を備える。アンテナ素子24は、給電素子であり、残るアンテナ素子21~23、25~27は、無給電素子である。そして、アンテナ素子24は、アンテナ素子21~23、25~27によって取り囲まれている。無給電素子であるアンテナ素子21~23、25~27のそれぞれには、可変容量素子であるバラクタダイオード（図示せず）が装荷されており、そのバラクタダイオードに印加する直流電圧を制御することにより、アレーアンテナ20は、適応ビーム形成が可能である。

【0023】

即ち、アレーアンテナ20は、無線装置30に含まれるバラクタダイオードに印加する直流電圧を変えることによって指向性を変えられる。従って、アレーアンテナ20は、電氣的に指向性を切換え可能なアンテナである。そして、アレーアンテナ20は、無線装置30に装着される。

【0024】

無線装置10と無線装置30との間で通信が行われる場合、電波は、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間を直接伝搬したり、中間物40による影響を受けて伝搬する。中間物40としては、反射物及び障害物が想定される。中間物40が反射物である場合、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から出射した電波は、中間物40によって反射されて無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬する。また、中間物40が障害物である場合、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から出射した電波は、中間物40によって回折されて無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬する。

【0025】

このように、電波は、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間を直接伝搬したり、中間物40による反射を受けて反射波として伝搬したり、中間物40による回折を受けて回折波として伝搬したりする。そして、電波は、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬する場合、直接伝搬成分、反射波成分及び回折波成分が混在しており、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬した電波がどのような成分により構成されるかによって無線装置10と無線装置30との間の伝送路の特性が決定される。

【0026】

この発明においては、無線装置10と無線装置30との間で通信が行なわれる場合、アレーアンテナ20の指向性を複数個に変えて時分割復信 (TDD: Time Division Duplex) 等により所定のデータが同一の周波数で無線装置10、30間で

送受信される。そして、無線装置10, 30は、アレーアンテナ20の指向性を複数個に変えたときの複数の電波の強度を示す受信信号プロファイルRSSIを生成し、その生成した受信信号プロファイルRSSIに基づいて秘密鍵を作成する。

#### 【0027】

秘密鍵が無線装置10, 30において生成されると、無線装置10, 30は、生成した秘密鍵により情報を暗号化して相手方へ送信し、相手方から受信した暗号化情報を復号して情報を取得する。

#### 【0028】

図2は、図1に示す一方の無線装置10の内部構成を示す概略ブロック図である。無線装置10は、信号発生部110と、送信処理部120と、アンテナ部130と、受信処理部140と、プロファイル生成部150と、鍵作成部160と、鍵一致確認部170と、鍵記憶部180と、鍵一致化部190と、暗号部200と、復号部210とを含む。

#### 【0029】

信号発生部110は、秘密鍵を生成するときに無線装置30へ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部120へ出力する。送信処理部120は、暗号部200から暗号化データを受けると、その受けた暗号化データに対して変調、周波数変換および増幅等を施してアンテナ部130から送信する。また、送信処理部120は、信号発生部110から所定の信号を受けると、所定の信号を所定の通信プロトコルであるIEEE802.11b（またはIEEE802.11g）の物理層を構成するデータフォーマットに含め、変調、周波数変換および増幅等を施してアンテナ部130から送信する。

#### 【0030】

アンテナ部130は、図1に示すアンテナ11からなり、送信処理部120からの信号を無線装置30へ送信し、無線装置30からの信号を受信して受信処理部140またはプロファイル生成部150へ供給する。

#### 【0031】

受信処理部140は、受信信号の増幅、多元接続、周波数変換及び復調等の受信系の処理を行なう。そして、受信処理部140は、受信処理を行なった信号を必要に応じて鍵一致確認部170、鍵一致化部190及び復号部210へ出力する。

#### 【0032】

プロファイル生成部150は、アレーアンテナ20の指向性を複数個に変えたときの複数の電波をアンテナ部130から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部150は、検出した複数の強度からなる受信信号プロファイルRSSIを生成して鍵作成部160へ出力する。

#### 【0033】

鍵作成部160は、プロファイル生成部150からの受信信号プロファイルRSSIに基づいて秘密鍵Ks1を作成する。そして、鍵作成部160は、作成した秘密鍵Ks1を鍵一致確認部170及び鍵一致化部190へ出力する。

#### 【0034】

鍵一致確認部170は、所定の信号を送信処理部120、アンテナ部130及び受信処理部140を介して無線装置30と送受信し、鍵作成部160によって作成された秘密鍵Ks1が無線装置30において作成された秘密鍵Ks2に一致するか否かを後述する方法によって確認する。そして、鍵一致確認部170は、秘密鍵Ks1が秘密鍵Ks2に一致すると確認したとき、秘密鍵Ks1を鍵記憶部180に記憶する。また、鍵一致確認部170は、秘密鍵Ks1が秘密鍵Ks2に不一致であることを確認したとき、不一致信号NMTTHを生成して鍵一致化部190へ出力する。

#### 【0035】

鍵記憶部180は、鍵一致確認部170及び鍵一致化部190からの秘密鍵Ks1を記憶する。また、鍵記憶部180は、記憶した秘密鍵Ks1を暗号部200及び復号部210へ出力する。なお、鍵記憶部180は、秘密鍵Ks1を一時的、例えば、無線装置30

との通信の間だけ記憶するようにしてもよい。

【0036】

鍵一致化部190は、鍵一致確認部170から不一致信号NMTHを受けると、後述する方法によって秘密鍵Ks1を秘密鍵Ks2に一致させる。そして、鍵一致化部190は、一致させた秘密鍵が秘密鍵Ks2に一致することを鍵一致確認部170における方法と同じ方法によって確認する。

【0037】

暗号部200は、送信データを鍵記憶部180に記憶された秘密鍵Ks1によって暗号して送信処理部120へ出力する。復号部210は、受信処理部140からの信号を鍵記憶部180からの秘密鍵Ks1によって復号して受信データを生成する。

【0038】

図3は、図1に示す他方の無線装置30の内部構成を示す概略ブロック図である。無線装置30は、無線装置10のアンテナ部130をアンテナ部220に代え、指向性設定部230を追加したものであり、その他は、無線装置10と同じである。

【0039】

アンテナ部220は、図1に示すアレーアンテナ20からなる。アンテナ部220は、送信処理部120からの信号を指向性設定部230によって設定された無指向性または指向性で無線装置10へ送信する。すなわち、アンテナ部220は、オムニアンテナまたは指向性アンテナとして機能し、送信処理部120からの信号を無線装置10へ送信する。また、アンテナ部220は、無線装置10からの信号を指向性設定部230によって設定された指向性で受信して受信処理部140またはプロファイル生成部150へ出力する。

【0040】

指向性設定部230は、アンテナ部220の指向性を設定する機能を持ち、無線装置10、30において秘密鍵Ks1、Ks2を生成するとき、後述する方法により、所定の順序に従ってアンテナ部220の指向性を順次切換え、またはアンテナ部220を無指向性に設定する。

【0041】

なお、無線装置30のプロファイル生成部150は、アレーアンテナ20の指向性を複数個に変えたときの複数の電波をアンテナ部220から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部150は、検出した複数の強度からなる受信信号プロファイルRSSIを生成して鍵作成部160へ出力する。

【0042】

図4は、図3に示す指向性設定部230の機能ブロック図である。指向性設定部230は、制御電圧発生回路231と、バラクタダイオード232とを含む。制御電圧発生回路231は、制御電圧セットCLV1～CLVn（nは自然数）を順次発生し、その発生した制御電圧セットCLV1～CLVnをバラクタダイオード232へ順次出力する。バラクタダイオード232は、制御電圧セットCLV1～CLVnに応じて無給電素子であるアンテナ素子21～23、25～27に装荷される容量を変え、アレーアンテナ20をオムニアンテナまたは指向性アンテナとして機能させる。すなわち、バラクタダイオード232は、制御電圧セットCLV1～CLVnに応じて無給電素子21～23、25～27のリアクタンス値を変えることによってアレーアンテナ20をオムニアンテナまたは指向性アンテナとして機能させる。この場合、制御電圧セットCLV1～CLVnの全てが0Vからなるとき、アレーアンテナ20は、オムニアンテナとして機能する。そして、バラクタダイオード232は、制御電圧セットCLV1～CLVnの複数の異なるセットに応じて、無給電素子21～23、25～27のリアクタンス値を順次変え、アレーアンテナ20の指向性を複数個に順次変える。

【0043】

図5は、図2及び図3に示す鍵一致確認部170の概略ブロック図である。鍵一致確認部170は、データ発生部171と、データ比較部172と、結果処理部173とを含む。なお、無線装置10、30の鍵一致確認部170は、同じ構成からなるが、図5におい

ては、秘密鍵 $Ks1$ が秘密鍵 $Ks2$ に一致することを確認する動作を説明するために、無線装置30においてはデータ発生部171のみを示す。

#### 【0044】

データ発生部171は、鍵作成部160から秘密鍵 $Ks1$ を受けると、秘密鍵 $Ks1$ が秘密鍵 $Ks2$ に一致することを確認するための鍵確認用データ $DCFM1$ を発生し、その発生した鍵確認用データ $DCFM1$ を送信処理部120及びデータ比較部172へ出力する。

#### 【0045】

この場合、データ発生部171は、秘密鍵 $Ks1$ から非可逆的な演算及び一方向的な演算等により、鍵確認用データ $DCFM1$ を発生する。より具体的には、データ発生部171は、秘密鍵 $Ks1$ または $Ks2$ のハッシュ値を演算することにより、鍵確認用データ $DCFM1$ を発生する。

#### 【0046】

データ比較部172は、データ発生部171から鍵確認用データ $DCFM1$ を受け、無線装置30のデータ発生部171で発生された鍵確認用データ $DCFM2$ を受信処理部140から受ける。そして、データ比較部172は、鍵確認用データ $DCFM1$ を鍵確認用データ $DCFM2$ と比較する。データ比較部172は、鍵確認用データ $DCFM1$ が鍵確認用データ $DCFM2$ に一致するとき、一致信号 $MTH$ を生成して結果処理部173へ出力する。

#### 【0047】

また、データ比較部172は、鍵確認用データ $DCFM1$ が鍵確認用データ $DCFM2$ に不一致であるとき、不一致信号 $NMTH$ を生成する。そして、データ比較部172は、不一致信号 $NMTH$ を鍵一致化部190へ出力し、不一致信号 $NMTH$ を送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

#### 【0048】

結果処理部173は、データ比較部172から一致信号 $MTH$ を受けると、鍵作成部160から受けた秘密鍵 $Ks1$ を鍵記憶部180へ記憶する。

#### 【0049】

図6は、図2及び図3に示す鍵一致化部190の概略ブロック図である。鍵一致化部190は、擬似シンδροーム作成部191と、不一致ビット検出部192と、鍵不一致訂正部193と、データ発生部194と、データ比較部195と、結果処理部196とを含む。

#### 【0050】

なお、無線装置10、30の鍵一致化部190は、同じ構成からなるが、図6においては、秘密鍵 $Ks1$ を秘密鍵 $Ks2$ に一致させる動作を説明するために、無線装置30においては擬似シンδροーム作成部191のみを示す。

#### 【0051】

擬似シンδροーム作成部191は、鍵一致確認部170のデータ比較部172から不一致信号 $NMTH$ を受けると、鍵作成部160から受けた秘密鍵 $Ks1$ のシンδροーム $s1$ を演算する。より具体的には、擬似シンδροーム作成部191は、秘密鍵 $Ks1$ のビットパターン $x1$ を検出し、ビットパターン $x1$ に対して検査行列 $H$ を乗算してシンδροーム $s1 = x1 H^T$ を演算する。そして、擬似シンδροーム作成部191は、ビットパターン $x1$ を鍵不一致訂正部193へ出力し、演算したシンδροーム $s1 = x1 H^T$ を不一致ビット検出部192へ出力する。

#### 【0052】

なお、これらの演算は、 $\text{mod } 2$ の演算であり、 $H^T$ は、検査行列 $H$ の転置行列である。

#### 【0053】

不一致ビット検出部192は、擬似シンδροーム作成部191からシンδροーム $s1$ を受け、無線装置30の擬似シンδροーム作成部191によって演算されたシンδροーム $s$

$2 = x_2 H^T$  を受信処理部140から受ける。そして、不一致ビット検出部192は、シンドローム  $s_1$  とシンドローム  $s_2$  との差分  $s = s_1 - s_2$  を演算する。

【0054】

なお、秘密鍵  $K_{s1}$ 、 $K_{s2}$  のビットパターンの差分（鍵不一致のビットパターン）を  $e = x_1 - x_2$  とすると、 $s = e H^T$  の関係が成立する。 $s = 0$  の場合、 $e = 0$  となり、秘密鍵  $K_{s1}$  のビットパターンは、秘密鍵  $K_{s2}$  のビットパターンに一致する。

【0055】

不一致ビット検出部192は、演算した差分  $s$  が0でないとき（即ち、 $e \neq 0$  のとき）、鍵不一致のビットパターンの差分  $e$  を鍵不一致訂正部193へ出力する。

【0056】

鍵不一致訂正部193は、擬似シンドローム作成部191からビットパターン  $x_1$  を受け、不一致ビット検出部192から鍵不一致のビットパターンの差分  $e$  を受ける。そして、鍵不一致訂正部193は、ビットパターン  $x_1$  から鍵不一致のビットパターンの差分  $e$  を減算することにより相手方の秘密鍵のビットパターン  $x_2 = x_1 - e$  を演算する。

【0057】

このように、鍵一致化部190は、秘密鍵  $K_{s1}$ 、 $K_{s2}$  の不一致を誤りと見なして誤り訂正の応用により秘密鍵  $K_{s1}$ 、 $K_{s2}$  の不一致を解消する。

【0058】

この秘密鍵を一致させる方法は、鍵不一致のビット数が誤り訂正能力以上である場合に鍵の一致化に失敗する可能性があるため、鍵一致化の動作を行なった後に鍵一致の確認を行なう必要がある。

【0059】

データ発生部194は、一致化後の秘密鍵のビットパターン  $x_2 = x_1 - e$  を鍵不一致訂正部193から受けると、 $x_2$  に基づいて鍵確認用データ DCFM3 を発生させ、その発生させた鍵確認用データ DCFM3 をデータ比較部195へ出力する。また、データ発生部194は、発生させた鍵確認用データ DCFM3 を送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

【0060】

なお、データ発生部194は、鍵一致確認部170のデータ発生部171による鍵確認用データ DCFM1 の発生方法と同じ方法により鍵確認用データ DCFM3 を発生する。

【0061】

データ比較部195は、データ発生部194から鍵確認用データ DCFM3 を受け、無線装置30で発生された鍵確認用データ DCFM4 を受信処理部140から受ける。そして、データ比較部195は、鍵確認用データ DCFM3 を鍵確認用データ DCFM4 と比較する。

【0062】

データ比較部195は、鍵確認用データ DCFM3 が鍵確認用データ DCFM4 に一致するとき、一致信号 MTH を生成して結果処理部196へ出力する。

【0063】

また、データ比較部195は、鍵確認用データ DCFM3 が鍵確認用データ DCFM4 に不一致であるとき、不一致信号 NMTH を生成する。そして、データ比較部195は、不一致信号 NMTH を送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

【0064】

結果処理部196は、データ比較部195から一致信号 MTH を受けると、鍵不一致訂正部193から受けた  $x_2 = x_1 - e$  を鍵記憶部180へ記憶する。

【0065】

このように、データ発生部194、データ比較部195及び結果処理部196は、鍵一致確認部170における確認方法と同じ方法によって一致化が施された鍵の一致を確認する。

## 【0066】

図7は、受信信号プロファイルRSSIの概念図である。図3および図4に示した指向性設定部230の制御電圧発生回路231は、各々が電圧V1～V6からなる制御電圧CLV1～CLVnを順次発生してバラクタダイオード232へ出力する。この場合、電圧V1～V6は、それぞれ、アンテナ素子21～23, 25～27に装荷される容量を変えるための電圧であり、0～20Vの範囲で変えられる。

## 【0067】

バラクタダイオード232は、パターンP1からなる制御電圧CLV1に応じてアレーアンテナ20の指向性のある1つの指向性に設定する。そして、アレーアンテナ20は、設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度WI1を検出する。

## 【0068】

次に、バラクタダイオード232は、パターンP2からなる制御電圧CLV2に応じてアレーアンテナ20の指向性を別の指向性に設定する。そして、アレーアンテナ20は、設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度WI2を検出する。

## 【0069】

以後、同様にして、バラクタダイオード232は、それぞれ、パターンP3～Pnからなる制御電圧CLV3～CLVnに応じてアレーアンテナ20の指向性を順次変える。そして、アレーアンテナ20は、各々設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度WI3～WInを順次検出する。

## 【0070】

そして、プロファイル生成部150は、強度WI1～WInからなる強度プロファイルを示す受信信号プロファイルRSSIを生成して鍵作成部160へ出力する。

## 【0071】

パターンP1～Pnによってアレーアンテナ20の指向性を複数個に順次切換えて無線装置30から無線装置10へデータを送信したとき、無線装置10のプロファイル生成部150が受信信号プロファイルRSSIを生成する。

## 【0072】

鍵作成部160は、プロファイル生成部150から受信信号プロファイルRSSIを受け、受信信号プロファイルRSSIから最大強度WImax(=WI6)を検出する。そして、鍵作成部160は、最大強度WImax(=WI6)によって受信信号プロファイルRSSIを規格化し、各強度WI1～WInを多値化する。鍵作成部160は、多値化した各値を検出し、その検出した各値をビットパターンとする秘密鍵Ks1またはKs2を作成する。

## 【0073】

図8は、所定の通信プロトコルであるIEEE802.11b（またはIEEE802.11g）の物理層およびMAC(Media Access Control)層のフォーマットを示す図である。物理層は、データを電気信号に変換し、実際の伝送を行なう階層である。そして、物理層は、IEEE802.11bおよびIEEE802.11gの両方に共通なデータフォーマットからなる。また、MAC層は、各無線装置間で信頼性の高いデータ伝送を行なう階層である。物理層は、PLCP(Physical Layer Convergence Protocol)プリアンブルと、PLCPヘッダとからなる。

## 【0074】

PLCPプリアンブルは、SYNC(SYNChronization field)信号と、SFD(Start Frame Delimeter)信号とからなる。また

、PLCPヘッダは、SIGNAL (SIGNAL or data rate) 信号と、SERVICE信号と、LENGTH信号と、CRC (Cyclic Redundancy Code) 信号とからなる。

【0075】

SYNC信号は、128ビットのデータ長を有する信号であり、同期の確立に使用される。SFD信号は、16ビットのデータ長を有する信号であり、PLCPプリアンプルの終了を示す。

【0076】

SIGNAL信号は、8ビットのデータ長を有する信号であり、MAC層のデータ速度を示す。SERVICE信号は、8ビットのデータ長を有する信号であり、機能拡張用として予約されている。LENGTH信号は、16ビットのデータ長を有する信号であり、MAC層のデータ長を示す。CRC信号は、16ビットのデータ長を有する信号であり、誤り検出に用いられる。

【0077】

また、MAC層は、PSDU (PLCP Service Data Unit) からなる。そして、PSDUは、48ビット以上のデータ長を有するMAC層のデータである。

【0078】

この発明においては、秘密鍵 $K_{s1}$ 、 $K_{s2}$ を生成する場合、無線装置10、30は、所定のデータを物理層に含め、アレーアンテナ20の指向性を変化させながら送信する。より具体的には、SYNC信号、SFD信号、SIGNAL信号、SERVICE信号、LENGTH信号およびCRC信号のうち、SYNC信号、SFD信号、SIGNAL信号およびSERVICE信号を複数のデータD0～D11から構成する。そして、複数のデータD1～D11は、所定のデータを分割したデータである。

【0079】

データD0は、36ビットのデータ長を有する。また、複数のデータD1～D11の各々は、11ビットのデータ長を有する。11ビットのデータ長に相当する時間長を期間T0とすると、複数のデータD1～D11の各々は、3ビットのデータ長に相当する期間T1と、8ビットのデータ長に相当する期間T2とに分割される。

【0080】

秘密鍵 $K_{s1}$ 、 $K_{s2}$ を生成する場合、データD0のデータ長に相当する期間T3、アレーアンテナ20をオムニアンテナとして機能させ、データD1～D11全体のデータ長に相当する期間T4、アレーアンテナ20を指向性アンテナとして機能させ、LENGTH信号およびCRC信号のデータ長に相当する期間T5、アレーアンテナ20をオムニアンテナとして機能させて所定のデータを送信する。

【0081】

そして、期間T4においてアレーアンテナ20を指向性アンテナとして機能させる場合、アレーアンテナ20の指向性が順次切換えられる。より具体的には、複数のデータD1～D11の各々の期間T1においてアレーアンテナ20の指向性が変化され、期間T2において、その変化された指向性でデータが送信される。従って、図8に示す例においては、アレーアンテナ20の指向性が11回変更されて所定のデータが送信される。

【0082】

所定のデータを受信する場合、所定のデータの送信時と同じように、期間T3、T5においてアレーアンテナ20をオムニアンテナとして機能させ、期間T4においてアレーアンテナ20を指向性アンテナとして機能させる。そして、所定のデータを受信時においては、複数のデータD1～D11の各々の期間T1においてアレーアンテナ20の指向性が変化され、その変化された指向性で受信した電波の強度が期間T2において検出される。従って、図8に示す例においては、所定のデータを受信時においても、アレーアンテナ20の指向性は、11回変更される。

【0083】



なお、期間T3においてアレーアンテナ20をオムニアンテナとして機能させるのは、通信の初期においては、AGC (Auto Gain Control) 機能を働かせ、データの受信レベルを最適値に調整する必要があるからである。また、期間T5においてアレーアンテナ20をオムニアンテナとして機能させるのは、次の理由による。物理層およびMAC層のデータ受信に誤りが生じると、確認応答 (=ACK信号) が返らず、再送状態が続いてしまう。したがって、これを防止するためにMAC層のデータに関連するLENGTH信号および物理層のデータ受信の成否を判定するCRC信号をオムニアンテナで送受信することにしたものである。

#### 【0084】

図9は、2つの無線装置10, 30間でデータを送受信する通常の方法の概念図である。また、図10は、2つの無線装置10, 30間におけるデータの再送の概念図である。更に、図11は、この発明の実施の形態において、2つの無線装置10, 30間でデータを送受信する方法の概念図である。

#### 【0085】

通常の方法においては、無線装置10は、アレーアンテナ20の指向性をリアクタンス変化パターン(1)に従って順次切換えて所定のデータDataを無線装置30へ送信する。そして、無線装置30は、所定のデータDataの受信を確認すると、確認応答Ackを無線装置10へ送信し、無線装置10は、アレーアンテナ20の指向性をリアクタンス変化パターン(1)に従って順次切換えて確認応答Ackを受信する。その後、無線装置10は、アレーアンテナ20の指向性をリアクタンス変化パターン(2)に従って順次切換えて所定のデータDataを無線装置30へ送信する。そして、無線装置30は、無線装置10から所定のデータDataを受信する(図9参照)。

#### 【0086】

しかし、このような通常の方法においては、アレーアンテナ20の指向性の変更によって図8に示すSYNC信号以降のデータを誤って受信した場合、物理層の同期は成立しているが、MAC層より上位の層の同期が成立しないため、確認応答Ackが返送されず、図10に示すように、アレーアンテナ20の指向性をリアクタンス変化パターン(1)に従って順次切換えて所定のデータDataを再送する動作が継続する。その結果、無線装置10, 30間において双方向の通信ができなくなる。

#### 【0087】

そこで、この発明においては、図11に示す方法で所定のデータDataを送受信する。すなわち、無線装置10は、アレーアンテナ20にオムニパターンを設定して所定のデータDataを無線装置30へ送信する。つまり、無線装置10は、アレーアンテナ20をオムニアンテナとして機能させて所定のデータDataを無線装置30へ送信する。

#### 【0088】

そして、無線装置30は、無線装置10からの所定のデータDataの受信を確認すると、確認応答Ackを無線装置10へ送信する。無線装置10は、アレーアンテナ20の指向性をリアクタンス変化パターン(1)に従って順次切換えて確認応答Ackを受信する。その後、無線装置10は、アレーアンテナ20の指向性をリアクタンス変化パターン(1)に従って順次切換えて所定のデータDataを無線装置30へ送信する。そして、無線装置30は、無線装置10から所定のデータDataを受信する(図11参照)。

#### 【0089】

図11に示す方法においては、無線装置10は、最初の送信において、通信が確立しているオムニパターンを使用するため、無線装置30から確認応答Ackを必ず受信できる。その結果、無線装置10, 30間における双方向の通信を確保できる。

#### 【0090】

そして、確認応答Ackは、図8に示す物理層のフォーマットからなるので、無線装置10は、アレーアンテナ20の指向性をリアクタンス変化パターン(1)に従って順次切換えて確認応答Ackを受信するとき、受信した確認応答Ackに含まれる複数のデータD1~D11に対応する複数の電波強度を検出できる。また、無線装置10は、確認応答

A c k の受信時におけるリアクタンス変化パターン (1) を使用してアレーアンテナ 20 の指向性を順次切換えて所定のデータ D a t a を無線装置 30 へ送信するので、無線装置 30 は、無線装置 10 において検出された複数の電波強度と同じ複数の電波強度を検出できる。

#### 【0091】

図 11 に示す方法によって所定のデータを無線装置 10, 30 間で 1 回送受信した場合、無線装置 10, 30 は、11 個の電波強度からなる強度プロファイル P I 11, P I 21 をそれぞれ検出する。そして、無線装置 10, 30 間における所定のデータの送受信を m (m は自然数) 回繰り返すことによって、無線装置 10, 30 は、m 個の強度プロファイル P I 11 ~ P I 1m, P I 21 ~ P I 2m をそれぞれ検出する。

#### 【0092】

そして、強度プロファイル P I 11 ~ P I 1m の全体に含まれる電波強度は、図 7 に示す n 個の電波強度 W I 1 ~ W I n に等しい。従って、無線装置 10, 30 間における所定のデータの 1 回の送受信によって、n 個の電波強度 W I 1 ~ W I n のうちの 11 個の電波強度 W I (i) ~ W I (i+10) (i=1~n-10) が検出される。

#### 【0093】

つまり、この発明においては、所定の通信プロトコルである I E E E 802.11b (または I E E E 802.11g) の物理層に所定のデータ D a t a を含めて無線装置 10, 30 間で送受信することを m 回繰り返すことによって n 個の電波強度 W I 1 ~ W I n が検出され、その検出された n 個の電波強度 W I 1 ~ W I n に基づいて秘密鍵 K s 1, K s 2 が生成される。

#### 【0094】

図 12 は、図 1 に示す 2 つの無線装置 10, 30 間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置 30 の送信処理部 120 は、k=1 を設定する (ステップ S1)。そして、指向性設定部 230 は、アレーアンテナ 20 をオムニアンテナとして機能させ、所定のデータ D a t a を無線装置 10 へ送信する (ステップ S2)。

#### 【0095】

続いて、無線装置 10 のアンテナ部 130 は、所定のデータ D a t a を受信し (ステップ S3)、その受信した所定のデータ D a t a を受信処理部 140 へ出力する。そして、受信処理部 140 は、所定のデータ D a t a の受信を確認すると、送信処理部 120 は、確認応答 (A c k 信号) をアンテナ部 130 から無線装置 30 へ送信する (ステップ S4)。

#### 【0096】

無線装置 30 の指向性設定部 230 は、アンテナ部 220 をオムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させ、アンテナ部 220 は、確認応答 (A c k 信号) を受信する (ステップ S5)。すなわち、アレーアンテナ 20 は、図 8 に示すデータ D0 をオムニアンテナとして受信し、指向性をパターン P k により 11 個に変化させながらデータ D1 ~ D11 を受信し、更に、L E N G T H 信号および C R C 信号をオムニアンテナとして受信する。

#### 【0097】

そして、アンテナ部 220 は、受信した複数のデータ D1 ~ D11 に対応する複数の電波をプロファイル生成部 150 へ出力する。プロファイル生成部 150 は、アンテナ部 220 からの複数の電波の強度プロファイル P I 1k を検出する (ステップ S6)。

#### 【0098】

次に、無線装置 30 の信号発生部 110 は、所定のデータを発生して送信処理部 120 へ出力し、送信処理部 120 は、所定のデータを物理層のデータ D1 ~ D11 に割り当て、オムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させたアンテナ部 220 を介して無線装置 10 へ所定のデータを送信する (ステップ S7)。すなわち、アンテナ部 220 は、図 8 に示すデータ D0 をオムニアンテナとして送信し、指向性をパ

ターンPkにより11個に変化させながらデータD1~D11を送信し、更に、LENGTH信号およびCRC信号をオムニアンテナとして送信する。

**【0099】**

無線装置10において、アンテナ部130は、無線装置30から所定のデータを受信する。(ステップS8)。そして、アンテナ部130は、受信した複数のデータD1~D11に対応する複数の電波をプロファイル生成部150へ出力する。プロファイル生成部150は、アンテナ部130からの複数の電波の強度プロファイルPI2kを検出する(ステップS9)。

**【0100】**

その後、無線装置30の送信処理部120は、 $k=k+1$ を設定し(ステップS10)、 $k=m$ であるか否かを判定する(ステップS11)。そして、 $k=m$ でないとき、ステップS2~S11が繰返し実行される。即ち、アレーアンテナ20の指向性パターンがパターンP1~Pmによってm個に変えられて、無線装置10のアンテナ部130と無線装置30のアンテナ部220との間で所定のデータを構成する電波が送受信され、強度プロファイルI11~I1m及びI21~I2mが検出されるまで、ステップS2~S11が繰返し実行される。

**【0101】**

ステップS11において、 $k=m$ であると判定されると、無線装置30において、プロファイル生成部150は、強度プロファイルI11~I1mに含まれる強度I11~I1nから受信信号プロファイルRSSI1を作成して鍵作成部160へ出力する。

**【0102】**

鍵作成部160は、受信信号プロファイルRSSI1から最大強度WImax1を検出し、その検出した最大強度WImax1によって受信信号プロファイルRSSI1を規格化し、強度I11~I1nを多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵Ks2を生成する(ステップS12)。

**【0103】**

また、無線装置10のプロファイル生成部150は、強度プロファイルI21~I2mに含まれる強度I21~I2nから受信信号プロファイルRSSI2を作成して鍵作成部160へ出力する。鍵作成部160は、受信信号プロファイルRSSI2から最大強度WImax2を検出し、その検出した最大強度WImax2によって受信信号プロファイルRSSI2を規格化し、強度I21~I2nを多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵Ks1を生成する(ステップS13)。

**【0104】**

次に、ステップS14において鍵一致の確認が行なわれる。即ち、無線装置10において、鍵作成部160は、秘密鍵Ks1を鍵一致確認部170へ出力する。鍵一致確認部170のデータ発生部171は、上述した方法によって鍵確認用データDCFM1を発生して送信処理部120及びデータ比較部172へ出力する。送信処理部120は、鍵確認用データDCFM1に変調等の処理を施し、アンテナ部130を介して無線装置30へ鍵確認用データDCFM1を送信する。

**【0105】**

そして、アンテナ部130は、無線装置30において発生された鍵確認用データDCFM2を無線装置30から受信し、その受信した鍵確認用データDCFM2を受信処理部140へ出力する。受信処理部140は、鍵確認用データDCFM2に所定の処理を施し、鍵一致確認部170のデータ比較部172へ鍵確認用データDCFM2を出力する。

**【0106】**

データ比較部172は、データ発生部171からの鍵確認用データDCFM1を受信処理部140からの鍵確認用データDCFM2と比較する。そして、データ比較部172は、鍵確認用データDCFM1が鍵確認用データDCFM2に一致しているとき、一致信号MTHを生成して結果処理部173へ出力する。結果処理部173は、一致信号MTHに応じて、鍵作成部160からの秘密鍵Ks1を鍵記憶部180に記憶する。

## 【0107】

一方、鍵確認用データDCFM1が鍵確認用データDCFM2に不一致であるとき、データ比較部172は、不一致信号NMTHを生成して送信処理部120及び鍵一致化部190へ出力する。送信処理部120は、不一致信号NMTHをアンテナ部130を介して無線装置30へ送信する。そして、無線装置30は、無線装置10において秘密鍵Ks1, Ks2の不一致が確認されたことを検知する。

## 【0108】

これにより、無線装置10における鍵一致の確認が終了する（ステップS14）。

## 【0109】

無線装置30においても、無線装置10と同じ動作によって鍵一致の確認が行なわれる（ステップS15）。

## 【0110】

ステップS14において、秘密鍵Ks1, Ks2の不一致が確認されたとき、無線装置10において、鍵一致化部190の擬似シンドローム作成部191は、鍵一致確認部170から不一致信号NMTHを受ける。そして、擬似シンドローム作成部191は、不一致信号NMTHに応じて、鍵作成部160から受けた秘密鍵Ks1のビットパターン $x_1$ を検出し、その検出したビットパターン $x_1$ のシンドローム $s_1 = x_1 H^T$ を演算する。

## 【0111】

擬似シンドローム作成部191は、演算したシンドローム $s_1 = x_1 H^T$ を不一致ビット検出部192へ出力し、ビットパターン $x_1$ を鍵不一致訂正部193へ出力する。

## 【0112】

一方、無線装置30は、ステップS11において無線装置10から不一致信号NMTHを受信し、その受信した不一致信号NMTHに応じて、シンドローム $s_2 = x_2 H^T$ を演算して無線装置10へ送信する。

## 【0113】

無線装置10のアンテナ部130は、無線装置30からシンドローム $s_2 = x_2 H^T$ を受信して受信処理部140へ出力する。受信処理部140は、シンドローム $s_2 = x_2 H^T$ に対して所定の処理を施し、シンドローム $s_2 = x_2 H^T$ を鍵一致化部190へ出力する。

## 【0114】

鍵一致化部190の不一致ビット検出部192は、受信処理部140から無線装置30において作成されたシンドローム $s_2 = x_2 H^T$ を受ける。そして、不一致ビット検出部192は、無線装置10で作成されたシンドローム $s_1 = x_1 H^T$ と無線装置30において作成されたシンドローム $s_2 = x_2 H^T$ との差分 $s = s_1 - s_2$ を演算する。

## 【0115】

その後、不一致ビット検出部192は、 $s \neq 0$ であることを確認し、鍵不一致のビットパターンの差分 $e = x_1 - x_2$ を $s = e H^T$ に基づいて演算し、その演算した鍵不一致のビットパターンの差分 $e$ を鍵不一致訂正部193へ出力する。

## 【0116】

鍵不一致訂正部193は、擬似シンドローム作成部191からのビットパターン $x_1$ と、不一致ビット検出部192からの鍵不一致のビットパターン $e$ とに基づいて、無線装置30において作成された秘密鍵Ks2のビットパターン $x_2 = x_1 - e$ を演算する。

## 【0117】

そして、データ発生部194、データ比較部195及び結果処理部196は、鍵一致確認部170における鍵一致確認の動作と同じ動作によって、一致化された鍵 $x_2 = x_1 - e$ の一致を確認する。

## 【0118】

これにより、鍵不一致対策が終了する（ステップS16）。

## 【0119】

無線装置30においても、無線装置10と同じ動作によって鍵不一致対策が行なわれる

(ステップS17)。

【0120】

ステップS14において、秘密鍵Ks1が秘密鍵Ks2に一致することが確認されたとき、またはステップS16において鍵不一致対策がなされたとき、暗号部200は、鍵記憶部180から秘密鍵Ks1を読み出して送信データを暗号化し、暗号化した送信データを送信処理部120へ出力する。そして、送信処理部120は、暗号化された送信データに変調等を施し、アンテナ部130を介して暗号化された送信データを無線装置30へ送信する。

【0121】

また、アンテナ部130は、暗号化された送信データを無線装置30から受信し、その受信した暗号化された送信データを受信処理部140へ出力する。受信処理部140は、暗号化された送信データに所定の処理を施し、暗号化された送信データを復号部210へ出力する。

【0122】

復号部210は、受信処理部140からの暗号化された送信データを復号して受信データを取得する。

【0123】

これにより、秘密鍵Ks1による暗号・復号が終了する(ステップS18)。

【0124】

無線装置30においても、無線装置10と同じ動作によって秘密鍵Ks2による暗号・復号が行なわれる(ステップS19)。そして、一連の動作が終了する。

【0125】

上述したステップS2～4に示す動作は、アレーアンテナ20をオムニアンテナとして機能させて無線装置10と無線装置30との間で通信を確立する動作である。また、ステップS4～S6に示す動作は、無線装置30において受信信号プロファイルRSSI1を生成するための電波を無線装置10のアンテナ11から無線装置30のアレーアンテナ20へ送信し、かつ、無線装置30において電波の強度プロファイルPI1kを検出する動作であり、ステップS7～S9に示す動作は、無線装置10において受信信号プロファイルRSSI2を生成するための電波を無線装置30のアレーアンテナ20から無線装置10のアンテナ11へ送信し、かつ、無線装置10において電波の強度プロファイルPI2kを検出する動作である。そして、所定のデータを構成する電波の無線装置10のアンテナ11から無線装置30のアレーアンテナ20への送信及び所定のデータを構成する電波の無線装置30のアレーアンテナ20から無線装置10のアンテナ11への送信は、アレーアンテナ20の指向性をパターンPkに従って変えながら交互に行なわれる。つまり、所定のデータを構成する電波は、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間で時分割通信により送受信される。

【0126】

従って、アレーアンテナ20の指向性をパターンPkに従って変えながら無線装置10のアンテナ11から無線装置30のアレーアンテナ20へ所定のデータを構成する電波を送信し、無線装置30において電波の強度プロファイルPI1kを検出した直後に、同じ所定のデータを構成する電波を無線装置30のアレーアンテナ20から無線装置10のアンテナ11へ送信し、無線装置10において電波の強度プロファイルPI2kを検出することができる。その結果、無線装置10、30間において同じ伝送路特性を確保して所定のデータを構成する電波を無線装置10、30間で送受信でき、電波の可逆性により電波の強度I11～I1nをそれぞれ電波の強度I21～I2nに一致させることができる。そして、無線装置10において作成される秘密鍵Ks1を無線装置30において作成される秘密鍵Ks2に容易に一致させることができる。

【0127】

また、所定のデータを構成する電波は、無線装置10、30間で時分割通信により送受信されるので、電波の干渉を抑制して1つのアレーアンテナ20を介して所定のデータを

構成する電波を無線装置10, 30間で送受信できる。

【0128】

更に、所定のデータは、所定の通信プロトコルであるIEEE802.11bおよびIEEE802.11gに共通な物理層に含めて無線装置10, 30間で送受信されるので、通信プロトコルがIEEE802.11bからIEEE802.11gへ変化してもデータフォーマットを変えずに秘密鍵Ks1, Ks2を生成できる。

【0129】

更に、無線装置30は、無線装置10からの確認応答(Ack信号)の受信時および所定のデータの無線装置10への送信時、同じパターンPkによってアレーアンテナ20の指向性を順次変更する(ステップS5, S7参照)。そして、同じパターンPkによってアレーアンテナ20の指向性を順次変更して無線装置10から確認応答(Ack信号)を受信する動作(ステップS5)および所定のデータを無線装置10へ送信する動作(ステップS7)は、k=mになるまで繰返し実行されるので、ステップS5, S7において、パターンPkに従ってアレーアンテナ20の指向性を順次変更することは、アレーアンテナ20の指向性を更新して無線装置10から確認応答(Ack信号)を受信し、その更新した指向性を維持して所定のデータを無線装置10へ送信することに相当する。

【0130】

このように、図11に示す方法によって所定のデータを無線装置10, 30間で送受信することによって所定のデータの再送が繰返されるのを防止し、無線装置10, 30間における双方向の通信を確保できる。すなわち、無線装置10, 30において同じ秘密鍵Ks1, Ks2を安定して作成できる。

【0131】

更に、アレーアンテナ20の指向性をパターンPkに従って変えながら無線装置10, 30間で所定のデータを構成する電波を送受信し、秘密鍵Ks1, Ks2を作成するための受信信号プロファイルRSSI1, RSSI2を生成するので、図1に示すようにアレーアンテナ20を装着した無線装置30の近傍に盗聴装置50が配置されていても、盗聴装置50による秘密鍵Ks1, Ks2の盗聴を抑制できる。

【0132】

即ち、盗聴装置50は、アンテナ11及びアレーアンテナ20から送信された電波をアンテナ51を介して受信するが、アレーアンテナ20は指向性をパターンPkに従って変えながら電波を送受信するので、アンテナ11とアレーアンテナ20との間で送受信される電波は、アンテナ11またはアレーアンテナ20とアンテナ51との間で送受信される電波と異なり、盗聴装置50は、無線装置30が送受信する電波と同じ電波を送受信できず、電波の強度プロファイルPI1kと同じ強度プロファイルを得ることができない。その結果、盗聴装置50は、秘密鍵Ks1, Ks2を盗聴することができない。

【0133】

従って、この発明においては、電氣的に指向性を切換え可能なアレーアンテナ20を盗聴装置50の近傍に配置された無線装置30に装着することを特徴とする。

【0134】

更に、鍵確認用データDCFM1~4は、秘密鍵Ks1, Ks2に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データDCFM1~4が盗聴されても秘密鍵Ks1, Ks2が解読される危険性を極めて低くできる。

【0135】

更に、シンドロームs1, s2は、秘密鍵Ks1, Ks2のビットパターンを示す鍵x1, x2に検査行列Hの転置行列H<sup>T</sup>を乗算して得られるので、シンドロームs1, s2が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

【0136】

なお、無線装置10, 30間で通信を行なう動作は、実際には、CPU(Central Processing Unit)によって行なわれ、無線装置10に搭載されたC

PUは、図12に示す各ステップS3, S4, S8, S9, S13, S14, S16, S18を備えるプログラムをROM (Read Only Memory) から読出し、無線装置30に搭載されたCPUは、図12に示す各ステップS1, S2, S5, S6, S7, S10, S11, S12, S15, S17, S19を備えるプログラムをROMから読出し、無線装置10, 30に搭載された2つのCPUは、その読出したプログラムを実行して図12に示すフローチャートに従って無線装置10, 30間で通信を行なう。

【0137】

従って、ROMは、無線装置10, 30間で通信を行なう動作をコンピュータ (CPU) に実行させるためのプログラムを記録したコンピュータ (CPU) 読取り可能な記録媒体に相当する。

【0138】

そして、図12に示す各ステップを備えるプログラムは、アレーアンテナ20の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置10, 30間における通信をコンピュータ (CPU) に実行させるプログラムである。

【0139】

上記においては、電氣的に指向性を切換え可能なアレーアンテナ20を無線装置30のみに装着すると説明したが、この発明においては、アレーアンテナ20は、無線装置10及び30の両方に装着されてもよい。

【0140】

即ち、この発明においては、アレーアンテナ20は、2つの無線装置10, 30のうち、少なくとも一方の無線装置に装着されていればよい。そして、アレーアンテナ20を装着した無線装置は、好ましくは、盗聴装置50の近傍に配置される。

【0141】

また、この発明においては、秘密鍵Ks1, Ks2の鍵長は、無線装置10, 30間の通信環境に応じて決定されてもよい。即ち、無線装置10, 30間の通信環境が盗聴し易い環境であるとき、秘密鍵Ks1, Ks2の鍵長を相対的に長くし、無線装置10, 30間の通信環境が盗聴しにくい環境であるとき、秘密鍵Ks1, Ks2の鍵長を相対的に短くする。

【0142】

更に、定期的に秘密鍵Ks1, Ks2の鍵長を変えるようにしてもよい。

【0143】

更に、無線装置10, 30間で送受信する情報の機密性に応じて秘密鍵Ks1, Ks2の鍵長を変えるようにしてもよい。即ち、情報の機密性が高いとき秘密鍵Ks1, Ks2の鍵長を相対的に長くし、情報の機密性が低いとき秘密鍵Ks1, Ks2の鍵長を相対的に短くする。

【0144】

そして、この鍵長は、アレーアンテナ20の指向性を変化させる個数、即ち、制御電圧CLV1~CLVnの個数により制御される。秘密鍵Ks1, Ks2は、検出された電波の強度I11~I1n, I21~I2nの個数からなるビットパターンを有し、電波の強度I11~I1n, I21~I2nの個数は、アレーアンテナ20の指向性を変化させる個数に等しいからである。つまり、制御電圧CLV1~CLVnの個数により秘密鍵Ks1, Ks2の鍵長を制御できる。

【0145】

このように、この発明においては、秘密鍵Ks1, Ks2の鍵長は、電氣的に指向性を切換え可能なアレーアンテナ20の指向性を変化させる個数によって決定される。

【0146】

更に、上記においては、2つの無線装置間において秘密鍵を生成する場合、即ち、1つの無線装置が1つの無線装置と通信する場合について説明したが、この発明は、これに限らず、1つの無線装置が複数の無線装置と通信する場合についても適用される。この場合、1つの無線装置は、通信の相手毎にアレーアンテナ20の指向性の切換パターンを変え

て秘密鍵を生成する。1つの無線装置は、アレーアンテナ20の指向性の切換パターンを1つに固定して複数の無線装置との間で秘密鍵を生成することも可能であるが（複数の無線装置の設置場所によって1つの無線装置との伝送路が異なるので、通信の相手毎に異なる秘密鍵を生成できる）、盗聴を効果的に抑制するには、通信の相手毎にアレーアンテナ20の指向性の切換パターンを変えて秘密鍵を生成するのが好ましい。

【0147】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【産業上の利用可能性】

【0148】

この発明は、秘密鍵の盗聴を抑制可能な無線通信システムに適用される。

【図面の簡単な説明】

【0149】

【図1】この発明の実施の形態による無線通信システムの概略図である。

【図2】図1に示す一方の無線装置の内部構成を示す概略ブロック図である。

【図3】図1に示す他方の無線装置の内部構成を示す概略ブロック図である。

【図4】図3に示す指向性設定部の機能ブロック図である。

【図5】図2及び図3に示す鍵一致確認部の概略ブロック図である。

【図6】図2及び図3に示す鍵一致化部の概略ブロック図である。

【図7】受信信号プロファイルRSSIの概念図である。

【図8】所定の通信プロトコルであるIEEE802.11b（またはIEEE802.11g）の物理層およびMAC層のフォーマットを示す図である。

【図9】2つの無線装置間でデータを送受信する通常の方法の概念図である。

【図10】2つの無線装置間におけるデータの再送の概念図である。

【図11】この発明の実施の形態において、2つの無線装置間でデータを送受信する方法の概念図である。

【図12】図1に示す2つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

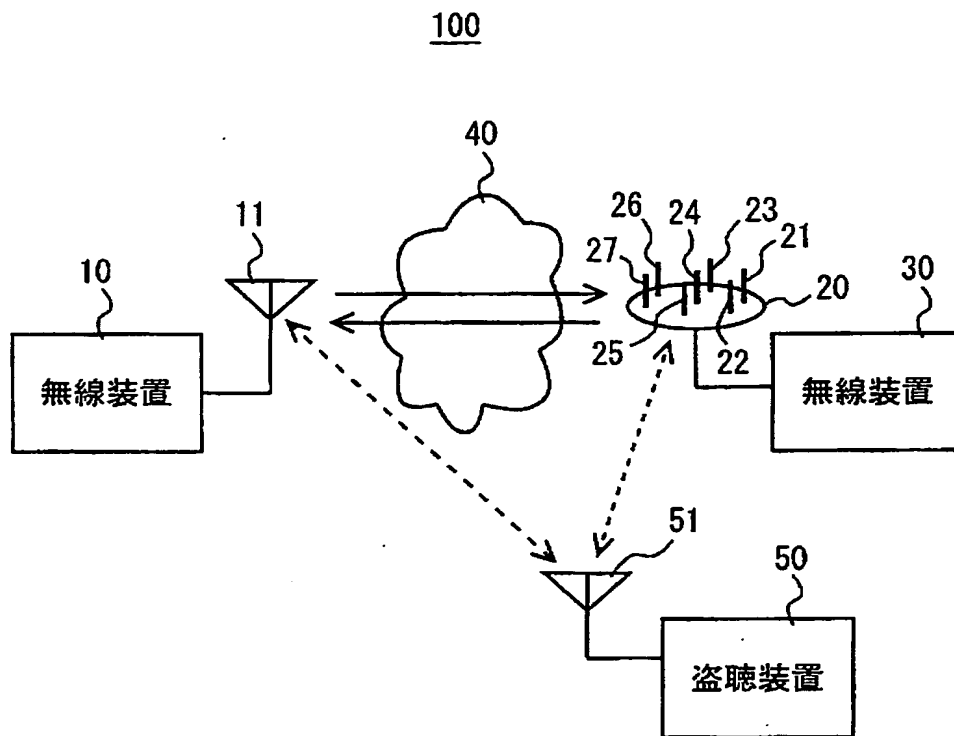
【符号の説明】

【0150】

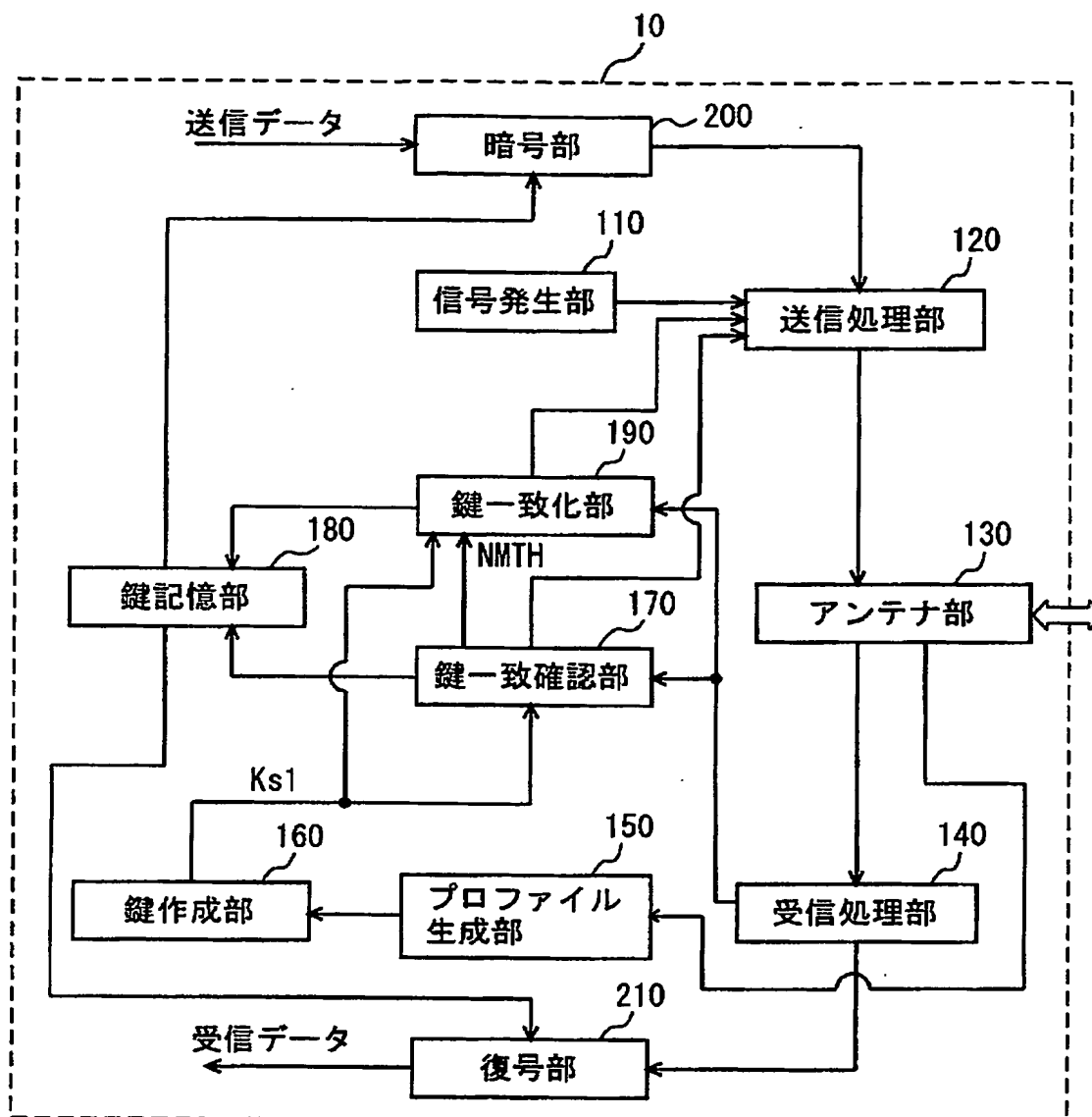
10, 30 無線装置、11, 51 アンテナ、20 アレーアンテナ、21～27  
アンテナ素子、40 中間物、50 盗聴装置、100 無線通信システム、110 信号発生部、120 送信処理部、130, 220 アンテナ部、140 受信処理部、150  
プロファイル生成部、160 鍵作成部、170 鍵一致確認部、171, 194  
データ発生部、172, 195 データ比較部、173, 196 結果処理部、180  
鍵記憶部、190 鍵一致化部、191 擬似シンドローム作成部、192 不一致ビット検出部、193 鍵不一致訂正部、200 暗号部、210 復号部、230 指向性設定部、231 制御電圧発生回路、232 バラクタダイオード。



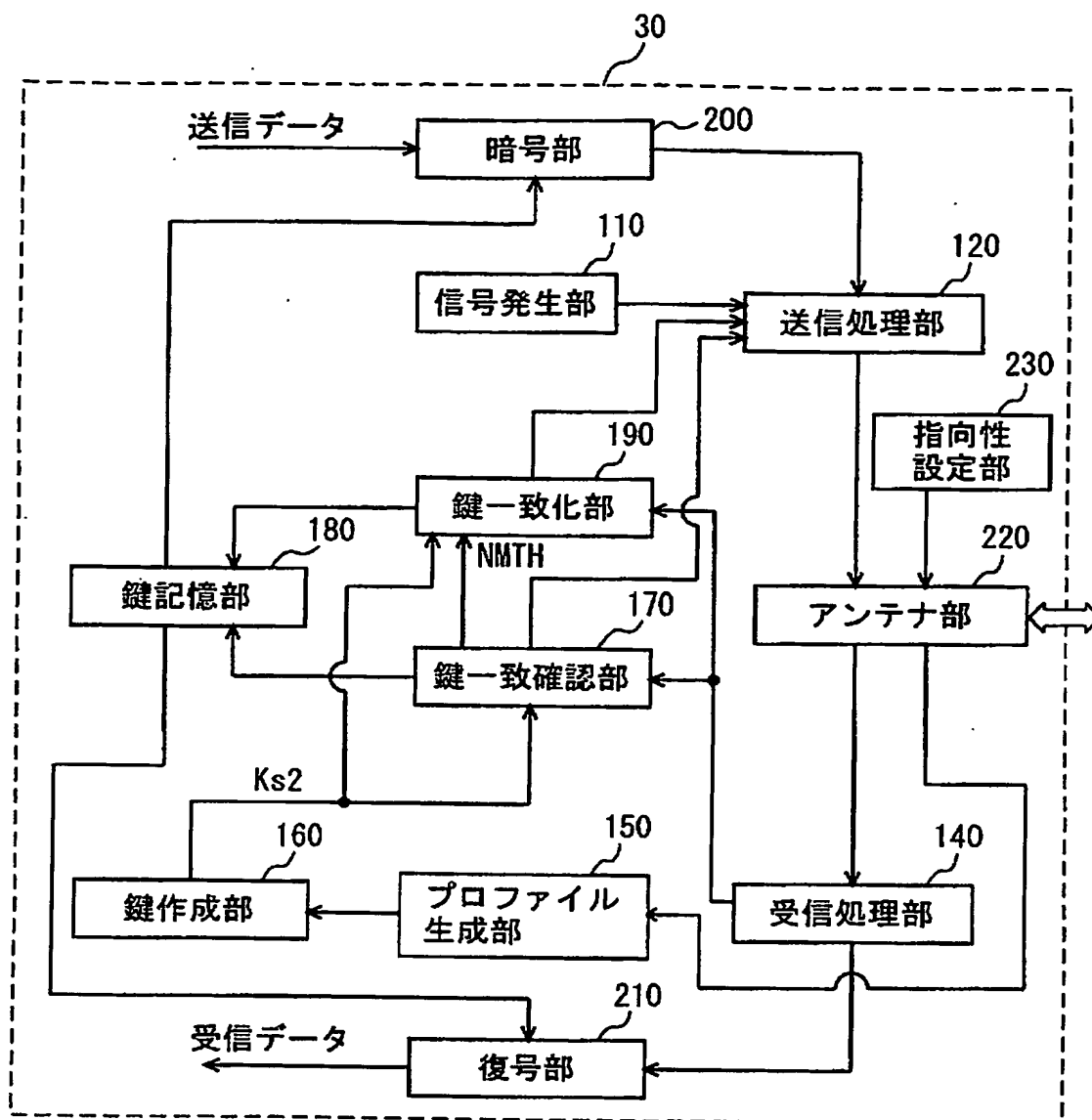
【書類名】 図面  
【図 1】



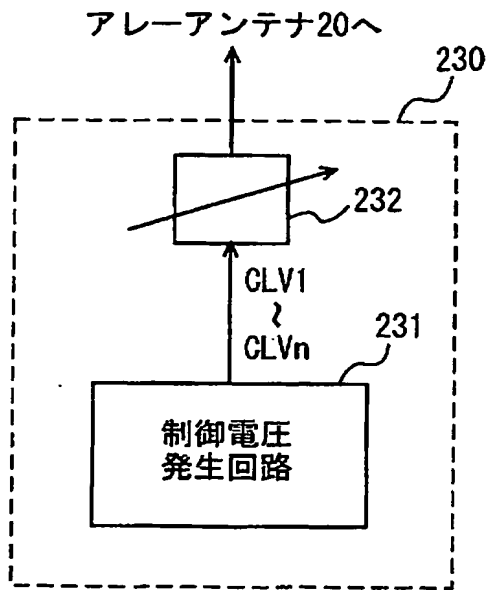
【圖 2】



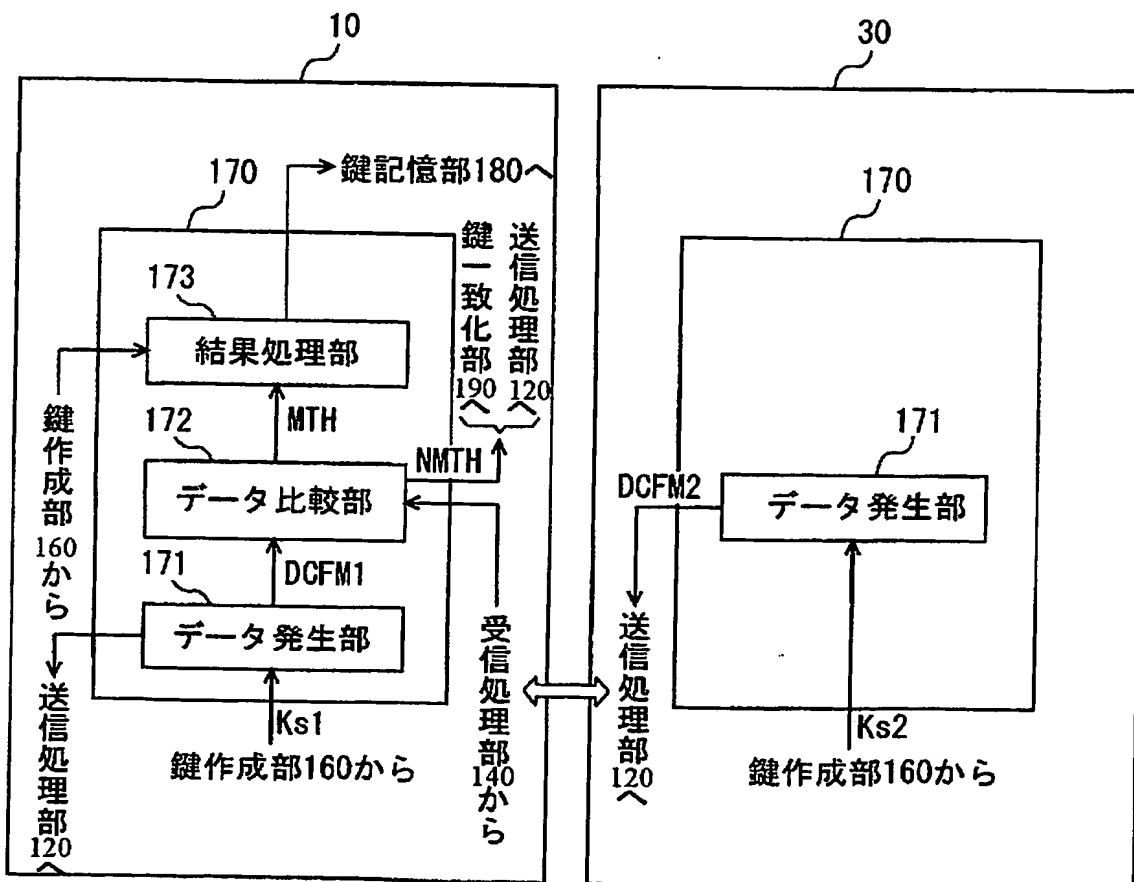
【図 3】



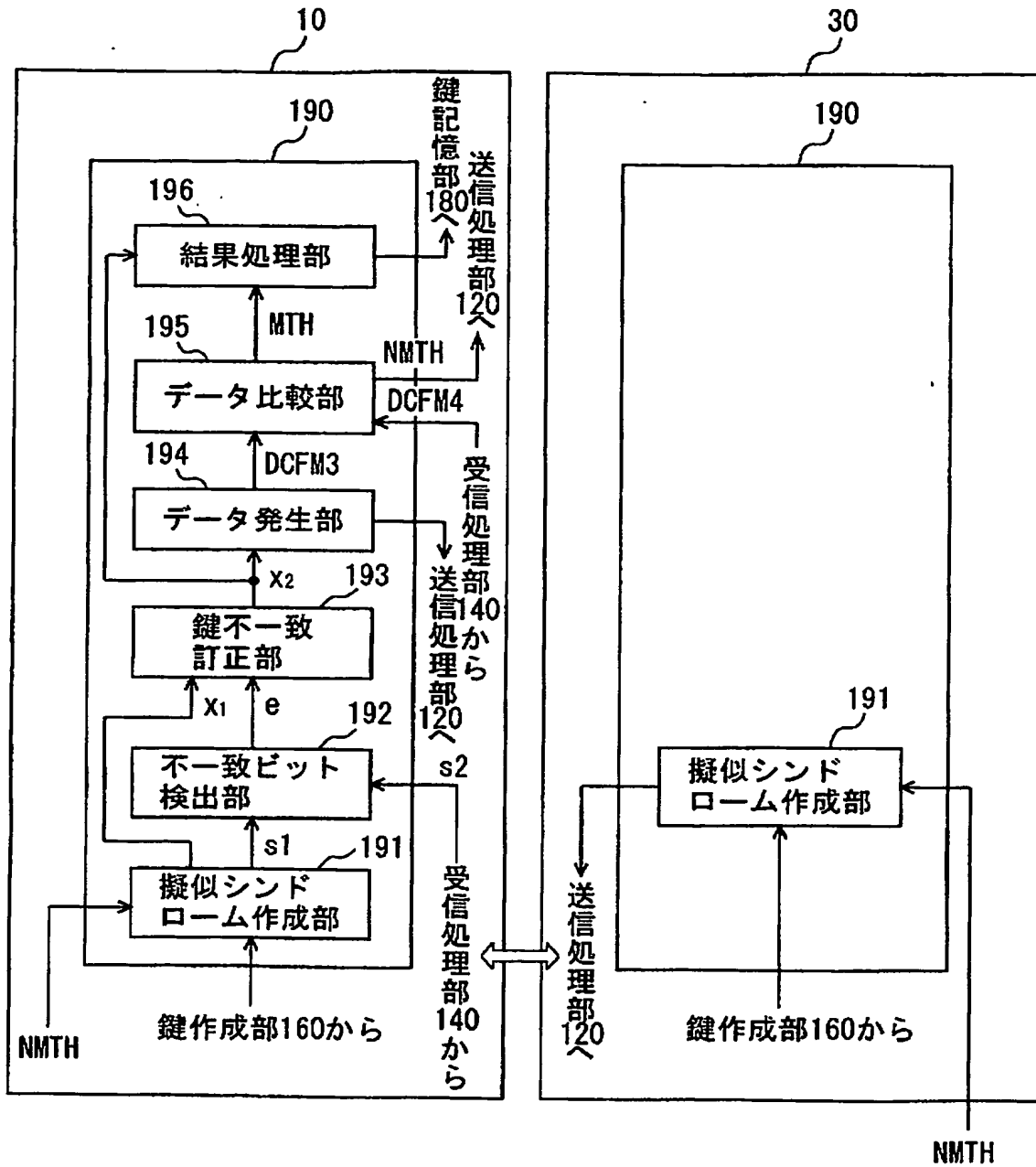
【図 4】



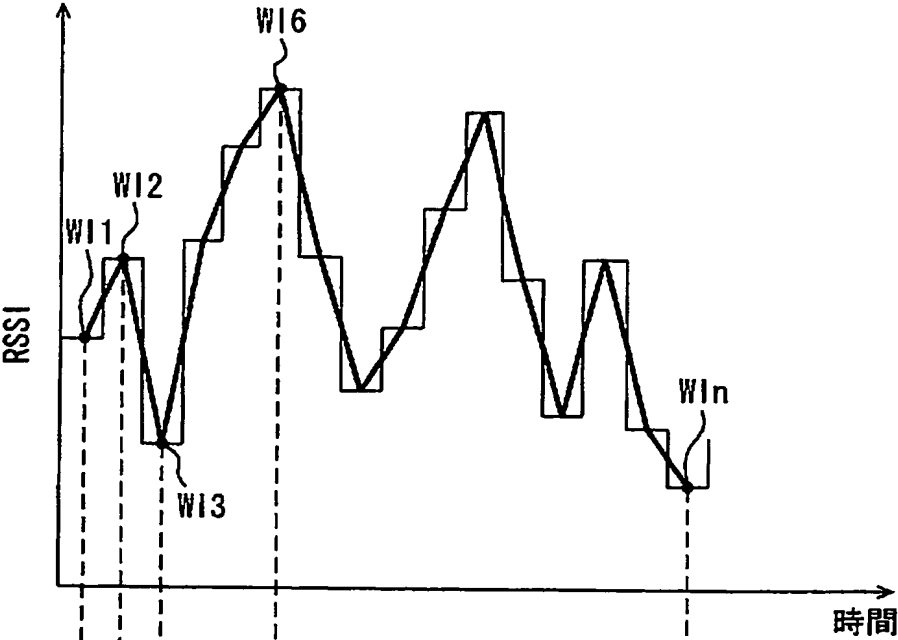
【図 5】



【図 6】

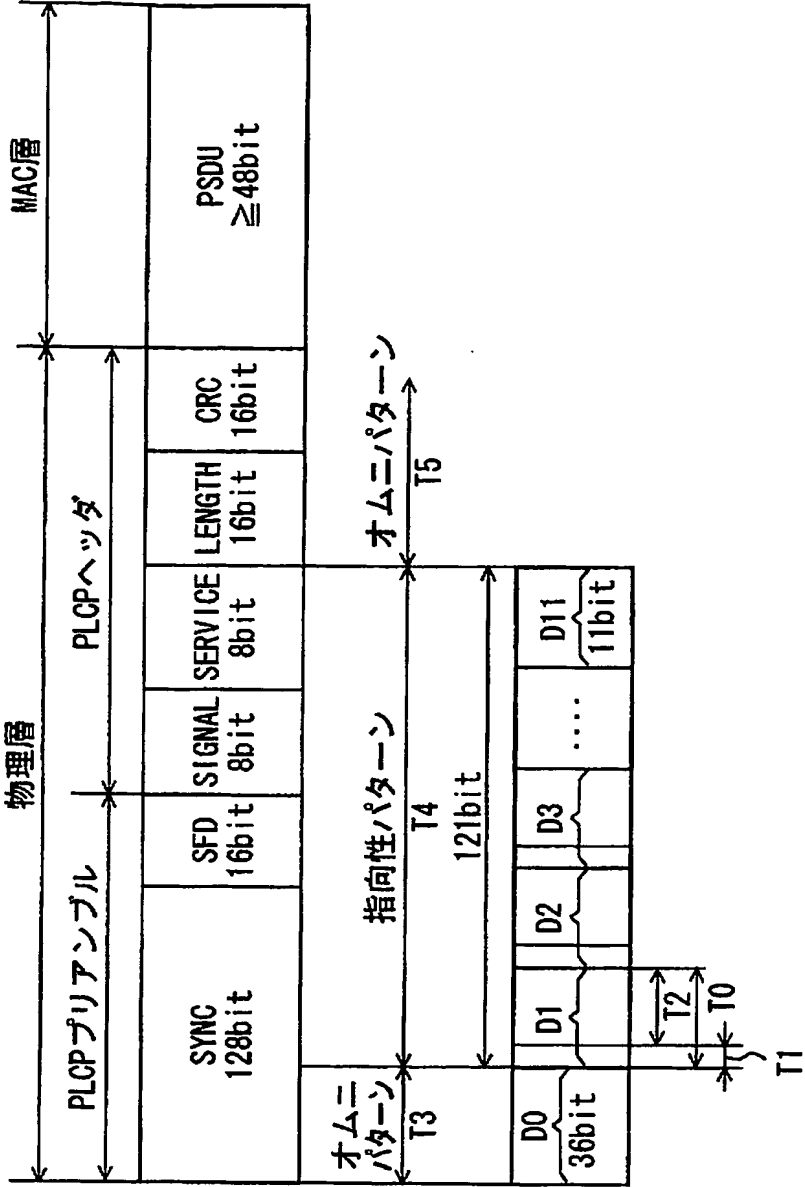


【図7】

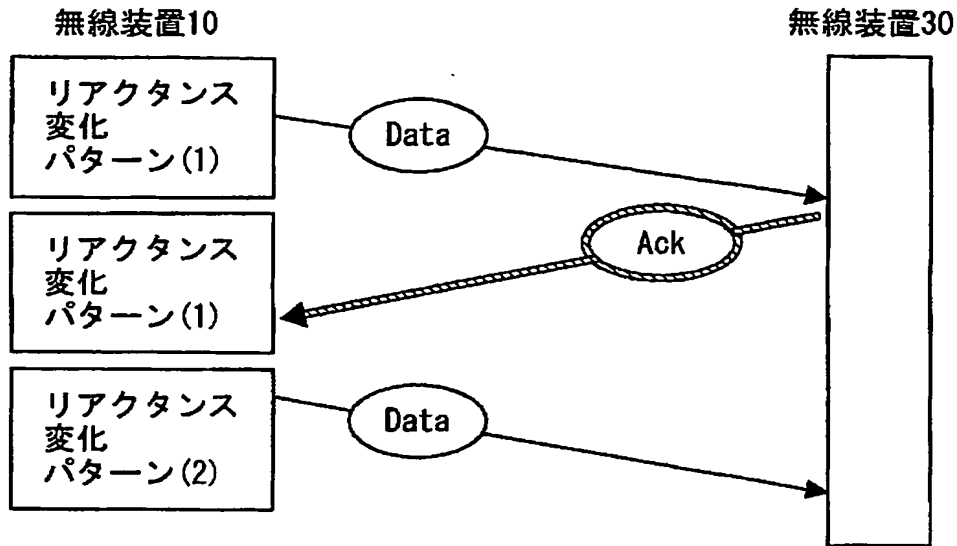


	P1	P2	P3	..	P6	.....	Pn
V1	0	1	2		0		0
V2	0	0	0		1		1
V3	1	0	0		0		0
V4	0	0	0	..	0	.....	2
V5	0	0	0		0		0
V6	0	0	0		0		1

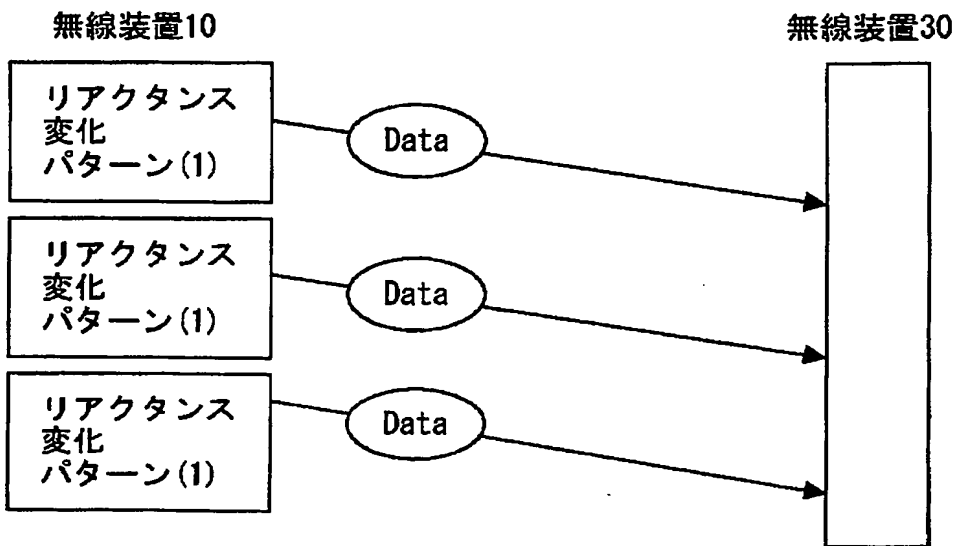
【図 8】



【図9】

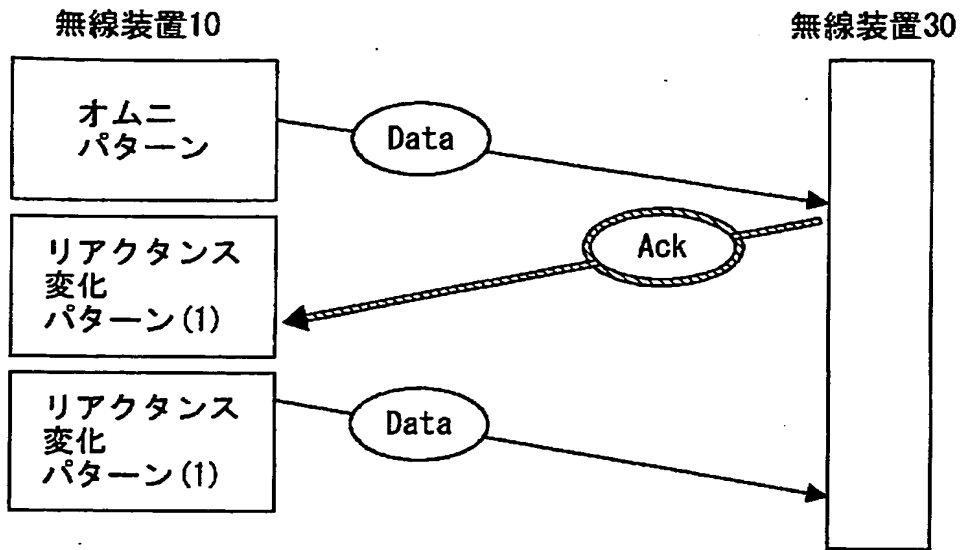


【図10】

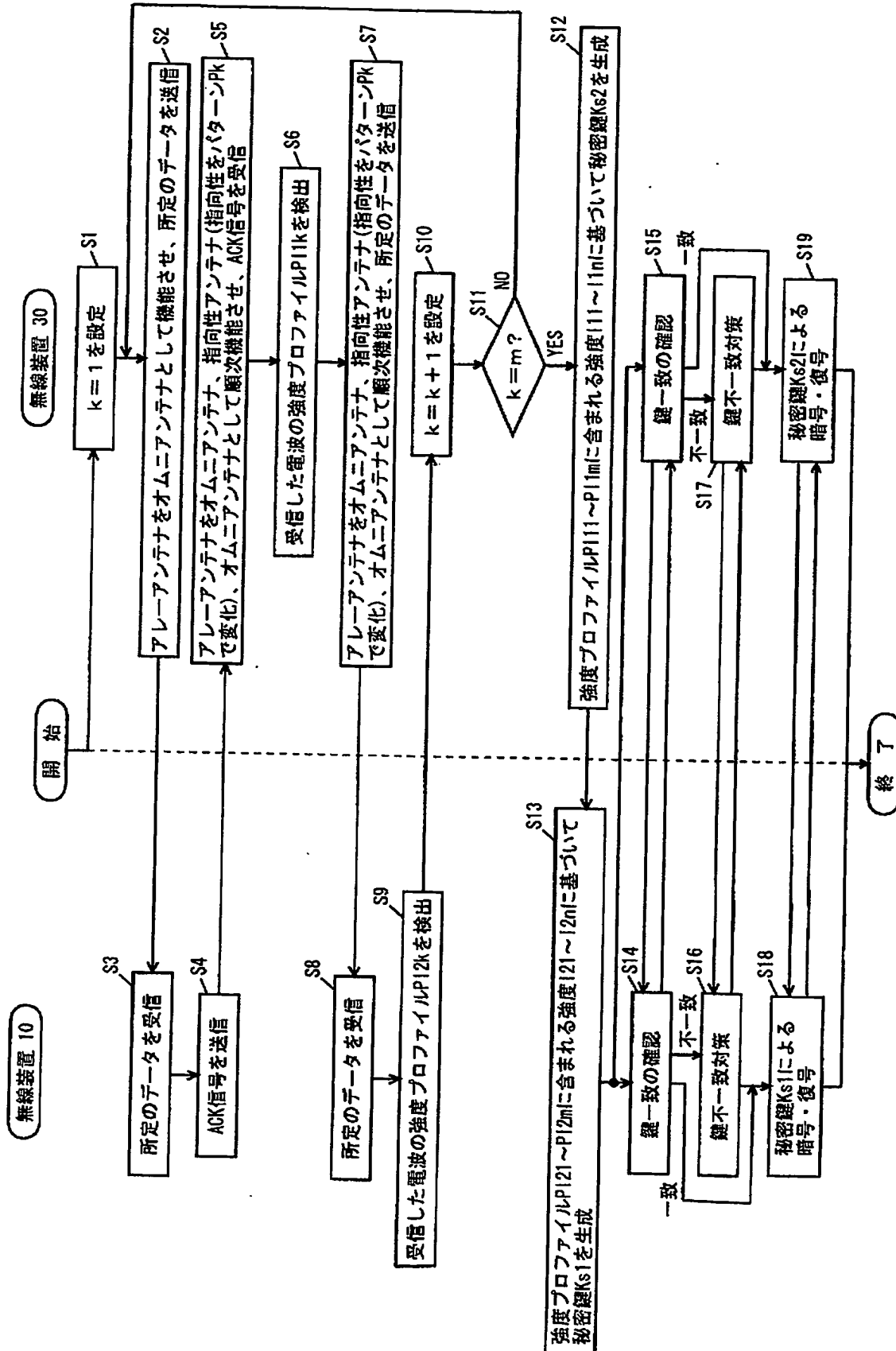




【図11】



【図12】



【書類名】 要約書

【要約】

【課題】 秘密鍵の盗聴を抑制可能な無線通信システムを提供する。

【解決手段】 無線通信システム 100 は、無線装置 10、30 と、アンテナ 11 と、アレーアンテナ 20 とを備える。無線装置 10 及び 30 は、アレーアンテナ 20 の指向性を複数個に変えながら所定の通信プロトコル (IEEE 802.11b) に従って所定の信号をアンテナ 11 及びアレーアンテナ 20 を介して相互に送受信する。そして、無線装置 10 及び 30 は、受信した複数の電波の強度を検出して複数の強度のプロファイルを示す受信信号プロファイル RSSI 1, 2 をそれぞれ作成する。無線装置 10 及び 30 は、それぞれ、受信信号プロファイル RSSI 1, 2 の複数の強度を多値化し、その多値化した複数の値をビットパターンとする秘密鍵 Ks 1, Ks 2 を作成する。

【選択図】 図 1

特願 2004-000533

出願人履歴情報

識別番号

[503027931]

1. 変更年月日

2003年 4月 4日

[変更理由]

住所変更

住 所

京都府京都市上京区今出川通烏丸東入玄武町601

氏 名

学校法人同志社

特願 2004-000533

出 願 人 履 歴 情 報

識別番号

[393031586]

1. 変 更 年 月 日

2000年 3月27日

[変更理由]

住所変更

住 所

京都府相楽郡精華町光台二丁目2番地2

氏 名

株式会社国際電気通信基礎技術研究所